LEADERS OF STUDENT`S COUNCIL
STATE UNIVERSITY OF TELECOMMUNICATIONS
SINCE 2009

Збірник матеріалів

XI Міжнародна науково-технічна конференція студенства та молоді

СВІТ ІНФОРМАЦІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

19 лютого 2021

Зміст

СИСТЕМИ АВТОМАТИЗОВАНОГО ПРОЕКТУВАННЯ В ТЕЛЕКОМУНІКАЦІЯХ

Аболонков Антон Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Серед інформаційних технологій автоматизація проектування займає особливе місце. По-перше, автоматизація проектування – синтетична дисципліна, її складовими частинами є багато інших сучасних інформаційних технологій. Так, технічне забезпечення систем автоматизованого проектування (САПР) засновано на використанні обчислювальних мереж і телекомунікаційних технологій.У сучасному виробництві широке поширення одержали **системи автоматизованого проектування (САПР, computer aided design)**, які дозволяють проектувати технологічні процеси з меншими витратами часу та засобів, зі збільшенням точності спроектованих процесів і програм обробки, що скорочує витрати матеріалів та час обробки, завдяки тому, що режими обробки також розраховуються та оптимізуються за допомогою ЕОМ. Проектування, при якому всі проектні рішення або їхня частина одержують шляхом взаємодії людини та ЕОМ, називають *автоматизованими* на відміну від ручного (без використання ЕОМ) або *автоматичного* (без участі людини на проміжних етапах). Система, що реалізує автоматизоване проектування, являє собою систему автоматизованого проектування (в англомовному написанні **CAD** System – Computer Aided Design System). САПР (або CAD) звичайно використовуються разом із системами автоматизації інженерних розрахунків і аналізу **CAE** (Computer-Aided engineering). Дані із CAD- систем передаються в **CAM** (Computer-Aided manufacturing) – систему автоматизованої розробки програм обробки деталей для верстатів.

CAE – автоматизоване конструювання, використання спеціального програмного забезпечення для проведення інженерного аналізу міцності та інших технічних характеристик компонентів, виконаних в системах автоматизованого проектування. Програми автоматизованого конструювання дозволяють здійснювати динамічне моделювання, перевірку та оптимізацію виробів і засобів їхнього виробництва.

CAM – автоматизоване виробництво. Термін використовується для позначення програмного забезпечення,

основною метою якого є створення програм для керування верстатами зі ЧПК (числове програмне керування). Вхідними даними CAM- системи є геометрична модель виробу, розроблена в системі автоматизованого проектування. У процесі інтерактивної роботи із тривимірною моделлю в CAM системі інженер визначає траєкторії руху різального інструменту по заготівлі виробу, які потім автоматично верифікуються, візуалізуються (для візуальної перевірки коректності) і обробляються постпроцесором для одержання програми керування конкретним верстатом.

Структура САПР. САПР складається з проектуючої і обслуговуючої підсистем. Проектуючі підсистеми безпосередньо виконують проектні процедури. Прикладами проектуючи підсистем можуть слугувати підсистеми геометричного тривимірного моделювання механічних об'єктів, виготовлення конструкторської документації, схемотехнічного аналізу, трасування з'єднань у друкованих платах. Огляд найбільш поширених САПР світових виробників.

AutoCAD – найвідоміший із продуктів компанії Autodesk, універсальна система автоматизованого проектування, що поєднує у собі функції двовимірного креслення й тривимірного моделювання. З'явився в 1982 році і був однієї з перших САПР, розроблених для PC. Швидко завоював популярність серед проектувальників, інженерів і конструкторів різних галузей промисловості завдяки демократичним цінам.

CATIA – система автоматизованого проектування французької фірми Dassault Systems. CATIA V1 була анонсована в 1981 році. У даний момент у світі використовуються дві версії – V4 і V5, які значно відрізняються між собою.

Pro/Engineer – CAD система високого рівня. Містить у собі всі необхідні модулі для твердотілого моделювання деталей і створення креслярської документації. Має убудовані можливості для проектування зварених конструкцій.

SolidWorks – продукт компанії SolidWorks Corporation, система автоматизованого проектування у трьох вимірах, працює під керуванням Microsoft Windows. Розроблена як альтернатива для двомірних програм САПР.

ADEM (Automated Design Engineering Manufacturing) – російська інтегрована CAD/CAM/CAPP-система, призначена для автоматизації конструкторсько-технологічної підготовки виробництва (КТПП).

КОМПАС – система автоматизованого проектування, розроблена російською компанією "АСКОН" з можливостями оформлення проектної й конструкторської документації

відповідно до стандартів серії ЕСКД і СПДБ (Система проектної документації для будівництва). Існує у двох версіях: Компас-Графік і КОМПАС-3D, відповідно призначених для плоского креслення і тривимірного проектування.

Використання САП на прикладі ВОЛЗ

Будівництво ВОЛЗ є складним, трудомісткий процесом, саме тому лише висока кваліфікація та досвід, здатна забезпечити можливість проектування, будівництво, експлуатацію та обслуговування ВОЛЗ у відповідності до високих вимог нормативних документів а також потреб Замовника. Для побудови лінії ВОЛЗ, потрібно пройти всі етапи, від розробки технічного завдання (ТЗ), отримання технічних умов (ТУ) до всього монтажу й виготовлення виконавчої документації та введення в експлуатацію ВОЛЗ. Послідовність розробки проекту і його склад при проектуванні ВОЛЗ в цілому такі ж, як при проектуванні інших інженерних систем. Проектна документація включає технічні розрахунки параметрів і характеристики обладнання, схеми прокладки і плани монтажу, обґрунтування топології мережі і архітектури внутрішньооб'єктного системи, специфікації компонентів системи, кошторис і іншу регламентну документацію. За допомогою САП можна:

- проектувати кабелі для подальшого використання;
- експертні висновки щодо технічної можливості прокладки лінії, монтажу обладнання для неї і їх експлуатації в конкретних умовах;
- підбір типу і довжини оптоволоконного кабелю; технічні розрахунки можливості та величини коефіцієнта загасання сигналу, інших показників, на які впливають конкретні умови прокладки і експлуатації.

Література:

1. Комп'ютерне моделювання систем та процесів. Методи обчислень. 1 частина [Електронний ресурс] – Режим доступу до ресурсу:https://web.posibnyky.vntu.edu.ua/fksa/2kvetnyj_komp%27yuterne_modelyuvannya_system_procesiv/t1/173..htm.

2.http://elib.hduht.edu.ua/bitstream/123456789/2819/1/%D0%9F%D0%BE%D1%81%D0%BE%D0%B1%D0%B8%D0%B5%20%D0%A1%D0%90%D0%9F%D0%A0%20%D0%A1%D0%B0%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%9D%D0%B5%D1%87%D0%B8%D0%BF%D0%BE%D1%80%D0%B5%D0%BD%D0%BA%D0%BE.pdf

3. Будівництво ВОЛЗ [Електронний ресурс] – Режим доступу до ресурсу: https://webpro.ua/building-an-focl.

4. Волоконно-оптична лінія передачі [Електронний ресурс] – Режим доступу до ресурсу:https://uk.wikipedia.org/wiki/%D0%92%D0%BE%D0%BB%D0%BE%D0%BA%D0%BE%D0%BD%D0%BD%D0%BE-%D0%BE%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B0_%D0%BB%D1%96%D0%BD%D1%96%D1%8F_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D1%96.

THE COMPARATIVE CHARACTERISTICS OF MEANS OF CONTINUOUS AUTOMATED DELIVERY OF EXECUTABLE CODE IN THE TASKS OF ENSURING THE QUALITY OF SOFTWARE PRODUCTS OF TELECOMMUNICATION SYSTEMS

Albul Oleksandr,
Sychov Stanislav
National Aerospace University
"Kharkiv Aviation Institute"

In the conditions of modern development in the period of globalization which is characterized by increase of level of openness of world economy, liberalization of economic activity there is an increase of a role of telecommunication services and the telecommunication equipment in practically all markets and in a life of people. , industries, countries and the world economy as a whole. In such conditions, the demand for software solutions related to the field of telecommunications is constantly growing.

In the development of such software solutions, the following stages are distinguished: collection and analysis of software requirements, development of software architecture, software development, testing and delivery of software to a productive environment. Because the software development process is time consuming and requires a lot of funding, it is advisable to optimize the processes throughout the development cycle. One of the optimization methods related to the stage of testing and delivery of software to a productive environment is the introduction of the concept of continuous integration (Continuous Integration) and continuous delivery (Continuous Delivery)[1, p.1].

Currently on the market there are many options for CI CD systems that have their advantages and disadvantages for implementation on various projects. Properly selected system will save time on software development and testing, prevent possible integration defects in the code when merging code from the branches of the version control system to the main branch, and thus save man-hours and develop more functionality per unit time [2, p.1].

The article provides a comparative description of existing CI CD systems. As a result, a conclusion is made about the feasibility of using the means of continuous automated delivery of executable code in the tasks of ensuring the quality of software products of telecommunication systems.

References:

1. Testing of telecommunication solutions: what is being done in the era of digital transformation // Telecommunications and IT [Electronic resource] - Access mode: https://shalaginov.com/2020/03/22/6988/ - 04.08.2020

2. GitLab Continuous Integration (GitLab CI/CD) [Electronic resource]. - Access mode:https://docs.gitlab.com/ce/ci/ – 05.08.2020

ОСОБЛИВОСТІ ОПОРНОЇ ТРАНСПОРТНОЇ МЕРЕЖІ NGN

Андрієнко Олеся Григорівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

В наш час поняття "транспортна мережа" відрізняється від звичного поняття "первинна мережа", а сфера застосування набагато ширша:

1. Мережа транспорту - це розвиток основної мережі під час переходу від комутації каналів до комутації пакетів.

2. Мережа транспорту - це опора сучасної мережі NGN (мережі наступного покоління), яка підтримує інтеграцію голосових, даних та мультимедійних послуг і базується на мережі IP (інтернет-протоколу).

3. В первинній мережі основною функцією є формування стандартного аналогового або цифрового каналу між двома мережевими точками, тоді як мережа передачі формує канал даних між двома точками підключення користувачів NGN.

4. Хоча принципи мережі передачі та первинної мережі схожі, NGN вводить свої особливості: замість типового каналу основної мережі використовується канал даних. Канал даних може бути встановлений на основі технології "віртуального каналу" , які можуть бути симетричними та асиметричними.

5. На відміну від мережі доступу, розгорнутої «на місці», мережа передачі побудована, як планувалось, відповідно до стратегії розвитку оператора.

Як відомо, основою мультисервісної мережі є універсальна мережа передачі, яка реалізує функції рівня передачі та управління рівнем обміну, маршрутизації та передачі інформації. Рівень передачі мультисервісної мережі побудований з використанням сучасних технологій, таких як IP, ATM (режим асинхронної передачі) та MPLS, які можуть забезпечити якість передачі інформації. Топологічна структура транспортного рівня мультисервісної мережі визначається топологічною структурою основної мережі, очікуваним обсягом трафіку в різних напрямках та функціональним використанням вузлів мережі.

Транспортна мережа є магістральною мережею, тому вона вимагає високих вимог щодо надійності, продуктивності та керованості. Мережа транспорту може включати:

- комутаційні вузли, які виконують функції передачі та комутації;
- термінальні вузли, що забезпечують абонентам доступ до мережі;
- контролери сигналізації, які виконують обробку інформації про сигнал, управління викликами та функції підключення;
- шлюзи, які дають змогу підключитись до традиційних мереж зв'язку (телекомунікації мережі, мережі передачі даних).

Розглянемо технологію MPLS - технологію швидкої комутації пакетів даних у багатоканальній мережі, засновану на використанні міток. MPLS був розроблений як спосіб побудови високошвидкісної IP-шини, але сфера її застосування не обмежується IP-адресою, але може бути розширена на будь-який трафік мережевого протоколу маршрутизації.

Традиційно основними вимогами до магістральних технологій є висока пропускна здатність, низька затримка та хороша масштабованість. Для постачальників послуг просто надання доступу до своїх IP-мереж вже недостатньо. Змінні потреби користувачів включають доступ до інтегрованих мережевих послуг, організацію віртуальних приватних мереж (VPN) та багато інших інтелектуальних послуг. З метою вирішення нових проблем була розроблена архітектура MPLS, яка забезпечує майже необмежену масштабованість, вищу швидкість обробки трафіку та безпрецедентну гнучкість в організації інших служб для побудови магістральних мереж.

Крім того, технологія MPLS дозволяє інтегрувати мережі IP та ATM, завдяки чому постачальники послуг можуть не тільки заощадити інвестиції в асинхронне обладнання передачі, але й отримати вигоду від спільного використання цих протоколів.

Однак архітектура MPLS відіграє важливу роль у зменшенні обсягу обробки, необхідного для кожного пакету даних на кожному маршрутизаторі в IP-мережі, тим самим додатково покращуючи продуктивність маршрутизатора. Не менш важливим є те, що MPLS, інформаційна основа розвитку інформаційних технологій, надає важливі нові можливості в наступних популярних сферах: підтримка якісної підтримки, дизайн трафіку, віртуальні приватні мережі, велика кількість підтримки протоколів тощо. Розглянемо ці можливості детальніше.

Література:

1. Гольдштейн А. Б. Технология и протоколы MPLS /А.Б. Гольдштейн, Б.С. Гольдштейн. – СПб. : БХВ-СанктПетербург, 2005. – 304 с

2. MPLS Fundamentals / Luc De Ghein. – Cisco Press, 2006. – 672 p
3. Вивек Олвейн Структура и реализация современной технологии MPLS..Руководство Cisco – М. : Вильямс, 2004. – 480 с

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЇ SDH В МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

Андрієнко Олеся Григорівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

На сьогоднішній день технологія SDH стала найпоширенішим та найпотужнішим інструментом створення високонадійних універсальних мереж передачі, на цій основі ви можете організувати спеціалізовані та мультисервісні телекомунікаційні мережі. Ця технологія досить поширена в мережах передачі. Вона широко застосовується у будівництві регіональних, національних та міжнародних транспортних мереж, відомчих мереж та операторів мобільного та фіксованого телефонного зв'язку.

Розвиток технології SDH полягає у вдосконаленні технічних рішень для задоволення нових вимог розвитку мережі. Основними методами розробки обладнання SDH є наступні:

- покращення швидкості агрегованих сигналів для досягнення більш високого рівня ієрархії. В рамках цієї галузі еволюцію можна вважати завершеною. Впровадження обладнання з електронною обробкою сигналу зі швидкістю вище 40 Гбіт / с є проблематичним та недоцільним;
- поліпшити ефективність передачі лінійних сигналів SDH на оптичних кабелях, тобто збільшити пропускну здатність системи передачі та довжину ділянки кабелю. Обладнання SDH останнього покоління оснащене оптичними підсилювачами та вбудованим обладнанням для стиснення спектра (WDM);
- термінологія розширеного інтерфейсу компонентного сигналу; окрім загального набору сигнальних інтерфейсів PDH (E1, EC, E4) та STM-N в традиційних системах SDH, існують також сигнальні інтерфейси, сформовані відповідно до протоколів ATM та IP, інтерфейси Ethernet, Fast Ethernet та Gigabit Ethernet, реле Frame , інтерфейс відеосигналу, сигнал xDSL тощо;
- узагальнення обладнання. Завдяки програмуванню та заповненню відповідного пристрою для заміни обладнання може виконувати функції будь-якого обладнання серії SDH. Уже є пристрої, які виконують функції мережевих вузлів.

- мініатюризація обладнання. Деякі дрібні вироби мають спрощений комплект обладнання. За винятком першої області, вдосконалення та розвиток обладнання SDH у всіх областях ще не завершено.

Відмінною рисою умовного SDH наступного покоління є функції, реалізовані на третьому, четвертому та другому (в порядку важливості) етапах розвитку. В даний час спостерігається тенденція переходу до пакетних даних. Це пояснюється зростаючим інтересом користувачів до послуг потрійної гри на основі Ethernet / MPLS та інших технологій комутації пакетів. Мережі наступного покоління мають усі переваги традиційних мереж SDH, вони мають більше функцій та певні показники якості зв'язку. Однак, вартість будівництва нової мережі передачі є дуже високою, а ресурси мережі SDH використовуються не до кінця.

Тому найкращим рішенням є оновлення існуючої мережі SDH та перетворення її на мережу SDH наступного покоління-NGSDH. Це дозволяє вирішувати майже всі ті самі проблеми, що й ATM або MPLS, без потреби повністю перебудовувати мережу. Основна технологія в NGSDH полягає у поєднанні базового GFP (загального фреймового протоколу) з VCAT (віртуальною конкатенацією).

Література:

1. Багатоканальний електрозв'язок та телекомунікаційні технології [Текст] / О. В. Лемешко, В. А. Лошаков, В. В. Поповський [та ін.]; за ред. проф. В. О. Поповського. – Харків: Компанія СМІТ, 2010. – Ч.1. – 468 с.

2. Бакланов, И. Г. NGN: принципы построения и организации [Текст] / И. Г. Бакланов. – М.:Эко-Трендз, 2008.

3. Сети следующего поколения NGN [Текст] / А. В. Росляков, С. В. Ваняшин, М. Ю. Самсонов [и др.]; под ред. А. В. Рослякова. – М. : Эко-Тренз, 2008. – 420 с

4. Recommendation ITU-T Y.110. Global Information Infrastructure principles and framework architecture.

ТРАНСПОРТНІ МЕРЕЖІ ETHERNET

Андрієнко Олеся Григорівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Високошвидкісні технології Ethernet (Gigabit та 10 Gigabit) є серйозною альтернативою іншим міським транспортним мережам NGN через наступні фактори:

- зростання вимог до смуги пропускання в зв'язку з появою нових типів додатків;
- висока концентрація абонентів в офісних та житлових будинках;

- зростаючий інтерес до масового ринку для роздрібних клієнтів через високу насиченість ринку корпоративних клієнтів та зниження рентабельності послуг на цьому ринку;
- низькі початкові інвестиції та експлуатаційні витрати;
- велика кількість професіоналів з досвідом роботи в Ethernet.

Рішення Ethernet забезпечує:

- мультисервісну та високонадійну інфраструктуру, яка підтримує договори про обслуговування, необхідні для відповідальних додатків;
- низькі витрати на розгортання мережі;
- винятково низьку вартість за Гбіт/с;
- стандартний інтерфейс з можливістю надання пакета послуг на одному порту клієнта (послуги мультиплексування);
- модульність і високу щільність агрегації - рішення для швидкого використання в районах з високою щільністю споживачів;
- відмінну масштабованість щодо кількості портів, продуктивності вузла та швидкості каналу (до 80 Гбіт/с);
- єдину технологію, механізми сигналізації та управління для всієї мережі;
- максимальну автоматизацію управління мережею та активація послуг, підтримка інструментів самообслуговування для клієнтів.

Зростаючі вимоги до місткості міських мереж та успіх існуючих операторів Ethernet чітко показують, що ця модель надання високошвидкісних телекомунікаційних послуг Ethernet у міських мережах NGN є конкурентоспроможною, затребуваною та вигідною для операторів зв'язку.

Типова міська мережа Ethernet заснована на трирівневій ієрархічній схемі і включає в себе ядро, рівень агрегації та рівень доступу.

Ядро мережі базується на високопродуктивних маршрутизаторах і забезпечує швидкісний трафік. Рівні агрегації побудовані на маршрутизаторах з низькою продуктивністю і забезпечують підключення на рівні доступу, реалізацію сервісу та агрегацію збору статистичної інформації. Залежно від розміру мережі, ви можете комбінувати рівні ядра та агрегації. Рівень ядра та агрегації забезпечує надмірність компонентів маршрутизатора, а також топологічну надмірність та дає змогу надалі надавати послуги у разі відмови окремих каналів та вузлів. Підтримувані надлишкові та захисні механізми комутації забезпечують час відновлення порівнянний із мережами SDH та мінімізують втрати трафіку під час аварії.

Рівень доступу зазвичай встановлюється в кільцевому або зірковому режимі на комутаторі для підключення корпоративних клієнтів та офісних будівель, а також для підключення домашніх клаєнтів та клієнтів такі як, невеликі офіси, домашні офіси). Комутатори також можна використовувати в зірковій топології та проміжній агрегації. На рівні доступу вживаються комплексні заходи безпеки для забезпечення ідентифікації та ізоляції клієнтів та захисту інфраструктури оператора. Мережа реалізує цілісний механізм забезпечення якості QoS та підтримує прозорі тунелі трафіку. Ефективна трансляція (багатоадресна передача) підтримується на всіх рівнях мережі, що важливо при реалізації таких сервісів, як TV over IP. Технологія ETTx є основою мережевої архітектури, яка забезпечує найширший спектр послуг на сьогоднішній день і швидко розгортається, коли нові сервіси стають доступними. Так, ринок домашніх користувачів ETTx - єдина технологія, яка дозволяє концепції Triple Play інтегрувати Інтернет, IP телефонію та інтерактивне телебачення (IPTV) в один програмний пакет, з достатнім зростанням для забезпечення перспективних послуг NGN.

Література:

1. Семенов Ю.В. Проектирование сетей связи следующего поколения. - СПб.: Наука и Техника, 2005. – 240 с.

2. Телекоммуникационные системы и сети. Том 3. – Мультисервисные сети / Под ред. проф. Шувалова В.П. – М.: Горячая линия-Телеком, 2005. – 592 с.

КЛАСИФІКАЦІЯ ТЕХНОЛОГІЙ РЕАЛІЗАЦІЇ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

Аніщенко Крістіна Ярославівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Якість виконання транспортних функцій мережею, забезпечуючи роботу цих телекомунікаційних служб, залежить від багатьох факторів і в першу чергу від правильної структуризації мережі, побудованої системи маршрутизації повідомлень в ній. На думку багатьох фахівців, VPN входить в трійку найважливіших технологій, які корпоративні користувачі збираються використовувати в найближчому майбутньому.

Значимість технології VPN для будь-яких компаній, а тим більше для малобюджетних організацій, обумовлена, перш за все, тими економічним вигодами, які пов'язані з її впровадженням. Існують різноманітні способи побудови віртуальних приватних мереж [1]. Серед усього іншого, ці способи відрізняються розподілом функцій по підтримці VPN

між корпоративною мережею і мережею загального користувача провайдера послуг VPN.

Класифікувати VPN можна за кількома основними параметрами:

- за типом використовуваного середовища, за способом реалізації,

- за призначенням, по рівню мережевого протоколу і ін.

Перш за все, всі віртуальні приватні мережі діляться на рис. 1:

- VPN, підтримувані обладнанням, яке встановлюється в приміщенні клієнта і служить для його підключення до магістралі сервіс-провайдера - так звані Customer - Provisioned VPN (CPVPN);

- VPN, підтримувані прикордонним обладнанням провайдера PE (Provider Edge) - так звані Provider-Provisioned VPN (PPVPN).

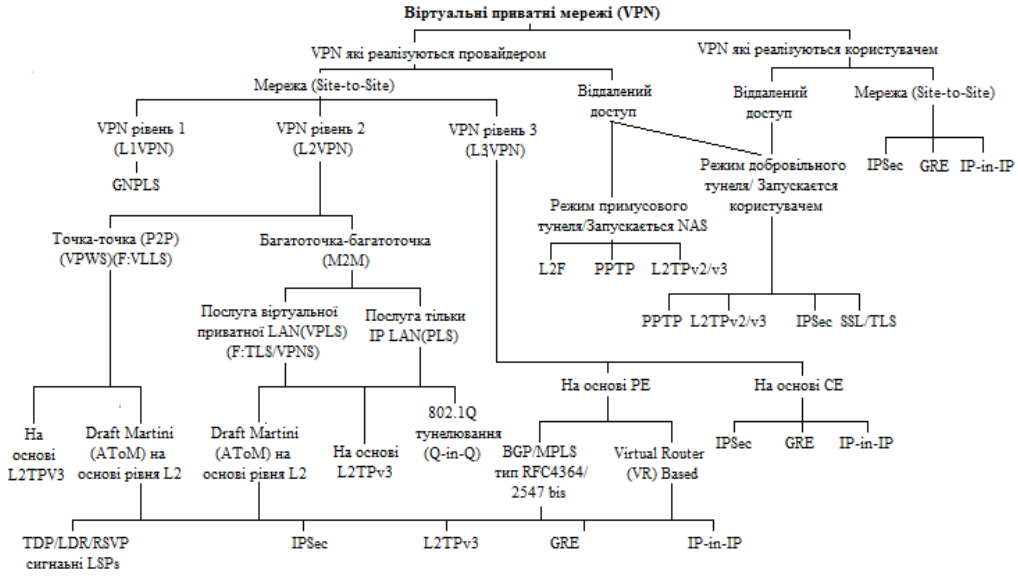


Рисунок 1.20 - Класифікація технологій реалізації VPN

І ті й інші VPN в свою чергу можна розділити на два класи в залежно від характеру організації зв'язку корпоративних користувачів [2]:

- для підключення декількох філій однієї організації в одну віртуальну приватну мережу (так звані site-to-site VPN);

- для підключення віддалених користувачів до центрального офісу або філії компанії (так звані remote access VPN).

Віртуальні мережі можуть бути реалізовані на базі протоколів моделі OSI різних рівнів: другого (канального) - L2VPN; третього (мережного) - L3VPN; п'ятого (сеансового) - L5VPN.

Для реалізації VPN 2-го рівня (L2VPN) можуть бути використані такі протоколи і технології:

1. Тунельний протокол 2-го рівня L2TP (Layer 2 Tunnelling Protocol) (стандарт IETF RFC 2661) - мережевий протокол тунелювання канального рівня, що поєднує в собі протокол L2F (layer 2 Forwarding). Дозволяє організовувати VPN із заданими пріоритетами доступу, проте не містить в собі засобів шифрування і механізмів аутентифікації.

2. Тунельний протокол «точка-точка» PPTP (point-to-point tunneling protocol) (стандарт IETF RFC 2637) - тунельний протокол типу «точка-точка», що дозволяє встановлювати захищене з'єднання за рахунок створення спеціального тунелю в стандартній, незахищеній мережі.

3. Послуга віртуальної приватної локальної мережі VPLS (Virtual Private LAN Service) забезпечує створення тунелів в мережі оператора зв'язку, які є незалежними від призначеного для користувача трафіку.

4. Послуга віртуального приватного дрота VPWS (Virtual Private Wire Service) - дозволяє організовувати прозорі з'єднання типу «точка-точка» через мережу MPLS.

Для реалізації VPN 3-го рівня (L3VPN) можуть бути використані такі протоколи і технології:

1) Набір протоколів IPsec (IP Security) - для забезпечення захистуданих, що передаються по міжмережевому протоколу IP, дозволяє здійснювати підтвердження автентичності та/або шифрування IP-пакетів.

2) Загальна інкапсуляція маршрутів GRE (Generic Routing Encapsulation) - протокол тунелювання мережевих пакетів, розроблений фірмою Cisco, забезпечує інкапсуляцію пакетів мережевого рівня моделі OSI в IP пакети.

3) Комбінована технологія BGP/MPLS – протокол прикордонного шлюзу BGP служить для прокладки маршрутів через опорну мережу MPLS.

4) Віртуальна приватна маршрутизації мережу VPRN (Virtual Private Routed Network) - використовуються для створення тунелів між вузлами транзитної мережі, а не між мережами що приєднуються через транзитну мережа.

Література:

1. Росляков, А. В. Виртуальные частные сети. Теория и практика применения/ А. В. Росляков. - М.: Эко-Трендз, 2016. - 304 с.

2. Miller S., Curran K., Lunney T. Traffic Classification for the Detection of Anonymous Web Proxy Routing // International Journal for Information Security Research (IJISR) . 2018. № 5(1). С. 538-545.

ОСНОВНІ АСПЕКТИ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІНТЕРНЕТ

Бабенко Єлизавета Костянтинівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У тезах розглянуто поняття, сутність та зміст інформаційної системи інтернет. Наведено та розкрито його основні ознаки. Проведено порівняльний аналіз та дослідження нормативно-правового статусу мережі. Висвітлено сучасний стан інформаційної системи інтернет та його значення для суспільства в цілому. Окреслено деякі проблемні питання, які можуть вплинути на доступність мережі широкому колу громадян чи призвести до монополізації ринку.

Наразі неможливо уявити наше життя без інтернету. Провівши вибіркове опитування людей різного віку, з'ясувалося, що лише незначна кількість респондентів спромоглася достеменно пояснити, що таке інтернет. Для більшості громадян інтернет – це типовий спосіб зв'язку, який використовується для міжособистісного спілкування, пошуку, розповсюдження та обміну інформацією, дистанційного навчання, роботи та інше. І це, зважаючи на дані 2019 року, відповідно до яких вже більшість людей планети користувалися інтернетом [1].

Загалом, вичерпне визначення поняття інтернету та його супутніх складових містилося лише в статті 1 Закону України «Про телекомунікації» [2, ст.1].

Отже, інтернет – це «всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами» [2, ст.1].

Вважаю, що саме це поняття дає можливість виокремити декілька основних ознак інтернету.

По-перше, він розглядається, як «інформаційна система загального доступу тобто це сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних» [2, ст.1].

По-друге, телекомунікаційна мережа загального користування - це мережа, вільний доступ до якої відкрито фактично для всіх, без винятку користувачів, які мають певне обладнання та технічні можливості, необхідні для реалізації власного права на отримання доступу для користування мережею інтернет [2, ст.1].

По-третє, адресний простір, який фактично становить сукупність адрес інтернет-мережі, являє собою символьний ідентифікатор доменів (іншими словами це конкретна адреса певної інтернет-сторінки) та відповідає загально-прийнятим

міжнародним стандартам [2, ст.1]. Наприклад, адресою інтернет-сторінки Державного університету телекомунікацій є http://dut.edu.ua.

Окремо варто звернути увагу на застосування мережею визначеного міжнародними стандартами інтернет-протоколу. Саме він дає можливість електронним пристроям користувачів з'єднуватися між собою як дротовим так і бездротовим способом. При цьому, такий стандарт забезпечує умови при яких, держави позбавлені можливості запроваджувати свої власні національні стандарти, які б відрізнялися від міжнародних, в іншому випадку їхні інформаційні мережі виключалися б із загальної [3, ст.262].

Зокрема, головною особливістю цієї мережі є те, що вона не має власника, а отже, згідно норм права не вважається об'єктом права, не є юридичною особою, а відповідно не може вважатися суб'єктом права. Окрім цього, жодна країна світу донині не має законодавчих актів, які б врегульовували діяльність саме інтернету [3, ст.262]. Існує низка нормативних актів, які регулюють лише окремі правовідносини пов'язані з інформаційною безпекою, захистом прав на об'єкти, які є інтелектуальною власністю, правові основи діяльності провайдерів та операторів.

З однієї сторони, сьогодні інтернет є вагомим інструментом для:

- реалізації народом права на свободу слова (наприклад, будь-хто може вести свій блог або розміщувати інформацію на інших ресурсах);
- оперативності отримання та донесення необхідної інформації до необмеженого кола осіб (наприклад, новини в засобах масової інформації, в тому числі через підписки);
- організації та проведення дистанційного навчання в умовах карантину, організація дистанційної роботи для бізнесу.

З іншої сторони інтернет цілком можна вважати засобом впливу на свідомість та формування світоглядів суспільства. Наприклад, для ведення так званої інформаційної війни, поширення «фейкової» інформації, пропаганди, шахрайства.

12 січня 2021 року Президент підписав Закон України «Про електронні комунікації» [4], яким оновлює поняття інтернет та прогнозує створення умов для надання рівного доступу до інтернету всім громадянам.

Варто звернути особливу увагу, що після дати набрання чинності цим нормативним актом (1 січня 2022 року), під поняттям інтернету необхідно буде розуміти «глобальну електронну комунікаційну мережу, що призначена для передачі

даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами» [4, ст.1].

Вважаю, що законодавець намагається розшити поняття інтернету та зробити його більш зрозумілим, але наразі воно виглядає складнішим для сприйняття пересічним громадянином в порівнянні з визначенням зазначеним в Законі України «Про телекомунікації» [2, ст.1].

Отже, поняття інтернет можна вважати складним, багатогранним та не достатньо дослідженим. Розвиток інформаційних технологій, впровадження новітнього обладнання розкриває нові можливості для користувачів інтернету. Та чи стане найближчим часом інтернет таким же доступним як був донині, а Україна «цифровою державною» покаже час. Адже, вже не одноразово правоохоронні органи намагалася пролобіювати так зване «право на стеження без рішення суду» і домогтися зобов'язання на законодавчому рівні встановлення дороговартісного обладнання необхідного для інтернет-стеження саме за рахунок провайдерів. Однозначно це призведе до подорожчання телекомунікаційних послуг, адже всі витрати операторів сплачують кінцеві споживачі.

Література:

1. Інтернет : матеріали з Вікіпедії – вільної енциклопедії // [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Інтернет#Назва.

2. Закон України «Про телекомунікації» від 18.11.2003 р. // Відомості Верховної Ради України. – 2004. - № 12. – Ст. 155.

3. Кормич Б.А. Інформаційне право : підручник / Б.А. Кормич. – Х. : Бурун і К, 2011. – 334 с.

4. Закон України «Про електронні комунікації» від 16.12.2020 р. [Електронний ресурс]. – Режим доступу: // https://itd.rada.gov.ua/billInfo/Bills/pubFile/409000.

РОЗРОБКА ПРОЕКТУ ТИПІЗОВАНОЇ МОДЕЛІ МУЛЬТИПЛЕКСОРНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Батушев Антон Борисович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Мета роботи – підвищення покаників якості мультисервісної мережі.

Предмет дослідження – моделі та алгоритми оцінки пропускної здатності ланок мультисервісної мережі.

Методи дослідження – методи натурного моделювання, теорії обчислювальних систем і масового обслуговування; методи теорії інформації та алгоритми складних систем, методи теорії системного аналізу, рекомендації та стандарти міжнародних організацій.

В роботі проведено огляд особливостей розвитку і планування мультисервісних мереж зв'язку, який показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл канального ресурсу на користь потоків заявок з малими потребами в ресурсі передачі нформації. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Виконаний аналіз особливостей розвитку і планування мультисервісних мереж зв'язку показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл канального ресурсу на користь потоків заявок з малими потребами в ресурсі передачі інформації. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Для обґрунтування процедури вибору конкретного сценарію необхідна розробка моделей, що реалізують ці сценарії, а також алгоритми.

Висновки

Виконаний аналіз особливостей розвитку і планування мультисервісних мереж зв'язку показав, що при спільному обслуговуванні неоднорідного трафіку комунікаційних додатків реального часу спостерігається неконтрольований оператором перерозподіл канального ресурсу на користь потоків заявок з малими потребами в ресурсі передачі інформації. Для усунення негативних наслідків цього явища пропонується застосовувати або резервування, або роздільне використання ресурсу ланок мережі. Для обґрунтування процедури вибору конкретного сценарію необхідна розробка моделей, що реалізують ці сценарії, а також алгоритмів розрахунку їх характеристик в розрахунку їх характеристик.

Література:

1.Вишневский В.М. Теоретические основы проектирования компьютерныхсетей. – М.: Техносфера, 2003. – 512с.

2.Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. – СПб:"БХВ- Петербург", 2005. – 304с.

МЕТОДИКА ПОБУДОВИ БЕЗПРОВІДНОЇ МЕРЕЖІ З ВИСОКОЮ ІНТЕНСИВНІСТЮ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Білокриницький Олег Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Мета роботи – проаналізувати можливість створення безпровідної мережі високої щільності та дослідити основні етапи розробки та налаштування мережі для забезпечення її високої пропускної спроможності та продуктивності.

На базі використання сучасного обладнання та програмного забезпечення в даний час цілком можливо побудувати на базі стандарту 802.11ac надійну, ефективну, захищену і стійку безпровідну мережу.

Розробка та налаштування мережі високої щільності

В роботі проаналізовано та досліджено процес розробки, налаштування та оцінки пропускної здатності безпровідної мережі з високою щільністю, який складається з наступних етапів:

- вибору необхідної кількості каналів;
- визначення пропускної здатності кожного каналу;
- визначення кількості користувачів на канал та необхідної кількості точок доступу у кожному каналі;
- вибору просторового фактору повторного використання частотних каналів;
- обчислення загальної пропускної здатності системи.

Висновки

1. З розвитком безпровідних технологій та появою точок доступу нового покоління з’явилася можливість створення складних високопродуктивних безпровідних мереж, які дозволять підвищити швидкість передачі, забезпечити високу щільність абонентів та задану надійність.

Література:

1. HP Ethernet Virtual Interconnect and Multitenant Device Context Enable Cloud Computing with multi-tenancy and simple Data Center Interconnection. [Електронний ресурс] – Режим доступу. – URL:http://h17007.www1.hpe.com/docs/814/factsheet.pdf

ПРИНЦИП РОБОТИ «РОЗУМНОГО БУДИНКУ» (IoT)

Богурський Артем Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Розумний будинок (або smart-house) — це сучасний продукт діджиталізації, що працює на основі штучного інтелекту.

Поняття розумного будинку з'явилося у XX столітті. До створення системи дистанційного керування доклав руку Нікола Теста, а перша система електронної автоматизації називалась «домашній комп'ютер Эхо IV», яка у 1966 році стала першим аналогом «розумного будинку».

Термін «розумний будинок» у 1984 році вигадала та ввела у вжиток Американська Асоціація Забудовників. Саме тоді почався спад цін на електроприлади, що уможливило будівництво офісів з високою функціональністю. Наприкінці XX століття почали з'являтися інтелектуальні побутові прилади і нові мультимедійні технології керування ними.

В переваги "smart home" входить його застосування для розумних побутових приладів, наприклад, для систем освітлення, опалення, кліматичних та музичних систем. Іншими елементами розумного дому можуть бути роботи-пилососи, інтелектуальні пральні та посудомийні машини, холодильники, камери спостереження або навіть кавові машини. Використовуючи їх, домовласники переслідують декілька цілей, найважливішими з яких є теми підвищення комфорту за рахунок автоматизації електронних приладів, а також енергозбереження, безпека.

Smart Home - це розумний дім, в якому прилади взаємодіють між собою і можуть управлятися за допомогою Інтернет-пристроїв, таких як смартфони, планшети і голосові помічники (розумні колонки). Простіше кажучи, розумний дім функціонує за принципом: введення, обробка, виведення.

На практиці із системою опалення це виглядає наступним чином:

1. **Введення**: за допомогою смартфона чи планшета запускається додаток. Відкривається користувацький інтерфейс та численні функції, серед яких може бути, наприклад, встановлення бажаної температури в приміщенні.

2. **Обробка**: частиною кожного розумного дому є так званий "центр управління розумним будинком", в якості якого може бути сервер з відповідним програмним та апаратним забезпеченням, спеціальний шлюз. Центр управління обробляє вихідні дані системи: періодично або за результатами якоїсь дії отримує параметри від інших пристроїв, аналізує їх і, в разі необхідності, надсилає команду іншому пристрою для виконання певної дії, наприклад увімкнення, вимкнення опалення або регулювання температури.

3. **Виведення**: після обробки відбувається виконання наказу приладом. У цьому випадку це опалювальна установка, яка транспортує такий об'єм гарячої води до радіаторів, який необхідний для досягнення бажаної Вами температури. Залежно від приладу виведення користувач додатку може бути поінформований про стан виконання наказу.

Взаємодія кінцевих пристроїв системи розумного будинку з центром управління здійснюється через дротові або бездротові протоколи передачі даних.

Перший варіант є більш надійним і захищеним з точки зору зовнішнього втручання, але останнім часом він не користується популярністю в зв'язку з необхідністю прокладання кабелів від кожного датчика чи виконавчого пристрою до центру управління. Зараз набирають популярність системи "розумний будинок" з застосуванням бездротових технологій, які мають ряд переваг, зокрема:

- автономність (відсутня прив'язка до точки підключення, датчики можуть переміщатись в межах приміщення, будинку, споруди);
- можливість інсталяції системи в оздоблене приміщення (немає необхідності в прокладанні кабелів);
- швидкість монтажу та налагодження системи;
- можливість розширення системи.

Але бездротові технології в системах "розумного будинку" мають також і недоліки, головними з яких є обмежений спектр радіочастот і його завантаженість, а також забезпечення енергоефективності кінцевих пристроїв для реалізації їх тривалої роботи від елементів живлення і обмеженої зони дії.

Найбільше поширення в системах "розумного будинку" набули наступні бездротові протоколи передачі: Zigbee, Z-Wave, Wi-Fi, BLE (Bluetooth Low Energy). Більшість бездротових протоколів використовує один частотний діапазон 2,4 ГГц, який у містах, в багатоквартирних будинках використовується для доступу смартфонів, планшетів, ноутбуків через Wi-Fi до мережі Інтернет. В місцях масового скупчення Wi-Fi пристроїв, часто виникає проблема з наявністю вільних частотних каналів.

Проблема обмеженої дистанції, на якій без втрат зв'язку можуть взаємодіяти бездротові кінцеві пристрої з центром управління, вирішується шляхом застосування mesh технології. Дана технологія передбачає підключення кінцевих пристроїв як безпосередньо до центру управління, так і через інші кінцеві пристрої, які мають підключення до мережі електроживлення.

Технологія mesh дозволяє розгортання бездротової мережі кінцевих пристроїв на великі площі.

На ринку почали з'являтися системи, які поєднують у собі охоронну, протипожежну системи та систему "розумного будинку".

Для України система розумного будинку є актуальною. Smart home уже впровадився в нові будинки Укрбуду. Є компанії CLAP, Ajax Systems які вже встановлюють свої нові технології в сучасні будинки, квартири та офіси.

Не мине багато часу, як в кожній квартирі, кожному будинку, всі електронні пристрої будуть не тільки елементами "розумного будинку", а й будуть використовувати штучний інтелект для підвищення комфорту та безпеки людей.

Література:

1. Розумний будинок — з чого він складається та чи потрібен вам [Електронний ресурс] – Режим доступу до ресурсу: https://nachasi.com/2018/06/25/smart-house-faq/.

2. Smart Home - розумний дім [Електронний ресурс] – Режим доступу до ресурсу: https://www.viessmann.ua/uk/zhytlovi-budynky/smarthome.html.

3. https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0268-2

НАСТУПНЕ ПОКОЛІННЯ БЕЗДРОТОВОГО ЗВ'ЯЗКУ WI-FI 6

Бойко Сергій Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі. Ознайомити слухачів з з новим стандартом бездротової мережі WiFi 6.

Мета дослідження. Поділити інформацію на наступні теми:

- Що таке Wi-Fi 6?
- Можливості Wi-Fi 6
- Основне призначення Wi-Fi 6
- Сфери, в яких Wi-Fi 6 може поліпшити продуктивність

Результати дослідження. Wi-Fi 6 (802.11ax) [2] - це стандарт бездротової мережі наступного покоління. Воно забезпечить Вам поліпшену швидкість Wi-Fi завдяки надійним з'єднанням, тому Ви зможете насолоджуватися безбуферною потоковою передачею, швидшими завантаженнями та додавати більше розумних домашніх пристроїв, не сповільнюючи роботу в Інтернеті.

У технології Wi-Fi кожна смуга частот (2,4 ГГц або 5 ГГц) складається з компонентних потоків. Саме за цими потоками

рухаються наші дані WiFi. Wi-Fi 5 і Wi-Fi 6 несуть найбільшу кількість потоків, таким чином забезпечуючи швидкість гігабітних Wi-Fi. Wi-Fi 6 збільшує кількість потоків до 12 в діапазонах 2,4 і 5 ГГц, тоді як Wi-Fi 5 має обмеження до 8 у двосмуговій конфігурації. Це збільшення потоків забезпечує вищу швидкість з'єднання, і Ваші клієнтські пристрої мають більше шляхів для зв'язку з вашим WiFi-маршрутизатором.

Потокове відео з роздільною здатністю 4K або 8K вимагає постійного високошвидкісного з’єднання. Завдяки поєднанню надшвидких процесорів, збільшеній пам'яті та збільшеній кількості радіопотоків, маршрутизатори WiFi 6 відповідають завданням потокової передачі декількох відео-сесій високої чіткості без заїкання, буферизації та інших надокучливих завдань, які ви побачите за допомогою старої технології Wi-Fi.

Wi-Fi 6 призначений для розумного будинку Пристрої розумного дому та додатки IoT [3] (інтернет пристроїв) поширюються. В результаті пристрої, підключені до Wi-Fi, у середньому будинку зростають із 10 пристроїв до 50 або більше. Кожна підключена до Wi-Fi лампочка, розумний перемикач, дверний замок, прилад або камера є навантаженням на вашу мережу. Wi-Fi 6 був розроблений, щоб мати змогу впоратися зі збільшенням кількості пристроїв, не впливати негативно на швидкість вашого Wi-Fi. Це призводить до безперебійного потокового передавання, забезпечуючи при цьому безперебійне підключення ліхтарів, вимикачів, термостатів та будь-якого іншого пристрою IoT, який ви можете додати до свого розумного будинку.

Wi-Fi 6 допоможе у галузях, що вимагають великої вимоги до пропускної здатності та вимог до високої щільності [1]. Такі галузі, як аеропорти, куди в будь-який момент проходить велика кількість користувачів, незалежно від того, чи вони використовують аеропорт як пункт пересадки або як місце відправлення, доступ до Wi-Fi для отримання інформації або розваг є необхідним. До додаткових галузей належать вищі навчальні заклади, такі як коледжі та університети, з їх широкою та різноманітною базою користувачів, програмами та пристроями. Розумні міста з різними департаментами, цивільними будівлями та громадянами мають певні вимоги, але всім потрібна краща ефективність роботи мережі, і список можна продовжувати. Будь-яка мережа, яка повинна забезпечувати підтримку додатків з високою пропускною здатністю в середовищі з високою щільністю, отримає найбільшу користь від Wi-Fi 6.

Література:

1. *“Netgear” [Електронний ресурс] - https://blog.netgear.com/*
2. *“IEEE 802.11ax” [Електронний ресурс] https://en.wikipedia.org/wiki/IEEE_802.11ax*
3. *“Wi-Fi Alliance“ [Електронний ресурс] - https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6*

DNS ЯК РОЗПОДІЛЕНА ІНФОРМАЦІЙНА СИСТЕМА

Виговський Олександр Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Доменні імена та IP-адреси можуть узгоджуватися як локальним хостом, так і централізованою службою. На ранніх стадіях розвитку Інтернету на кожному хості вручну створювався текстовий файл із відомим іменем хосту. Файл складався з ряду рядків, кожен з яких містив одну пару "IP-адреса - доменне ім'я", наприклад 102.54.94.97 - rhino.acme.com.

У міру зростання Інтернету зростали і хост-файли, і стало необхідним створити масштабоване рішення з роздільною здатністю імен.

Рішенням стала спеціальна послуга - Система доменних імен (DNS) - це централізована служба, заснована на розподіленій базі даних "доменне ім'я - IP-адреса". Служба DNS використовує у своїй роботі протокол клієнт-сервер. Визначає DNS-сервери та DNS-клієнти. DNS-сервери розміщують розподілену базу даних зіставлення, а клієнти DNS просять сервери перетворити доменне ім'я на IP-адресу.

Система доменних імен (DNS) спрямована на встановлення глобальної відповідності між символічними іменами хостів та їх IP-адресами. Завданням DNS є перетворення символічних імен в IP-адреси і навпаки, коли кількість веб-сайтів зростає в геометричній прогресії.

На думку користувача, хост в системі - це той хост, де знаходиться користувач. Однак, крім хостів і маршрутизаторів, сервери імен (система DNS) RFC 2136, 2137, 2152 також відіграють важливу роль програми розподіленого управління базами даних, що використовуються для зберігання символічних назв мереж і хостів та їх IP-адрес. Найпоширенішою програмою для вирішення таких проблем є BIND (Інтернет-ім'я Беркела Domen). Іноді для цього ставлять інший автомобіль.

IP-адреси дуже ефективні, але користувачам краще запам'ятовувати символи, ніж цифри. Тому цифрова адреса буде замінена текстовою формою - доменним іменем. DNS

використовує ієрархічну схему розподілу доменних імен для децентралізації управління різними частинами простору імен.

Доменні імена мають ієрархічну структуру і складаються з ряду елементів, розділених крапками. Ці точки спочатку ідентифікують мережу (справа наліво), потім ідентифікують окремі вузли хосту, а іноді і служби хостів (WWW, FTP тощо). Правильний елемент - це домен верхнього рівня, який базується на географічних особливостях (наприклад, uk (Великобританія), ua (Україна), ru (Росія)) або тип організації.

Для зіставлення доменних імен з IP-адресами використовується спеціальна база даних, яка містить IP-адресу кожного доменного імені. Такі бази даних підтримуються спеціальними серверами імен, і доступ до них можна отримати за допомогою спеціальних протоколів DNS. Доменні імена верхнього рівня реєструються в одному з центрів реєстрації, головним чином InterNIC (Інформаційний центр Інтернет-мережі), Інформаційний центр Інтернету (формування, реєстрація та стратегічний розвиток Інтернету, включаючи реєстрацію доменних імен) (США).

Домен верхнього рівня розділений на кілька субдоменів, і реєстратор домену верхнього рівня фіксує розташування сервера імен для кожного з цих субдоменів. Реєстратори можуть додавати нові імена до своїх субдоменів, не звертаючись до сервера імен верхнього рівня. Наприклад, домен верхнього рівня ua розділений на піддомени kyiv.ua, lviv.ua, kharkiv.ua та ck.ua. Субдомен ck.ua у Черкасах працює у мережі UANET. Піддомен, визначений Університетом ЧДТУ, реєструє свій сервер імен у мережі. Однак очевидно, що простим оновленням свого локального сервера імен субдомен fitis та субдомен ks601 Школи інформаційних технологій та систем можуть бути призначені кожному хосту в мережі.

DNS-сервер домену повинен підтримувати таблицю відповідностей між IP-адресами та символічними іменами всіх вузлів у домені.

Кожен вузол домену повинен знати лише IP-адресу свого сервера домену і надсилати йому всі запити на перетворення символічного імені вузла в IP-адресу. Якщо сам сервер домену не може відповісти на запит (наприклад, запитувана IP-адреса іншого хоста домену), він може зв’язатися з кореневим DNS-сервером, щоб дізнатися IP-адресу потрібного сервера домену, а потім зв’язатися з ним. Сервер домену. Природно, що DNS-сервер може запам'ятовувати результати таких пошуків, і коли ви переглядаєте ту саму інформацію, не повторюйте шлях знову і негайно надсилайте кешовані дані.

База даних DNS-сервера містить інформацію про адреси всіх DNS-серверів у цьому домені (для підвищення надійності, як правило, кожен домен підтримує принаймні два DNS-сервери, і вони повинні знаходитися в різних підмережах IP), список псевдонімів (той самий вузол) Може мати кілька символічних назв), а також список поштових серверів для домену.

Література:

1. Основи сучасних комп'ютерних технологій: Навчальний посібник / під. ред. Хомоненко. - СПб.: КОРОНА, 2005. – 240 с.

2. Тюрін Ю.М., Макаров А.А. Статистичний аналіз даних на комп'ютері. Під ред. В.Е. Фігурнова. М.: ИНФРА-М, 1998.. – 592 с.

3. Савельєв А.Я., Сазонов Б.А., Лук'янов Б.А. Персональний комп'ютер для всіх. Зберігання та обробка інформації. Т.1 М.: Вища школа, 2001.

СИСТЕМИ ЗВ’ЯЗКУ НА ОСНОВІ IP-ТЕХНОЛОГІЙ

Виговський Олександр Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

IP-телефонія має достатньо переваг і незабаром буде запущена по всій нашый країні. VoIP - це система зв'язку, що забезпечує передачу голосового сигналу через Інтернет або будь-якою іншою IP-мережею. Сигнал по каналу зв'язку зазвичай передається цифровим способом, а потім передається (стискається) перетворюється (для усунення надмірності).

Давно минули часи, коли оператори боялися користуватися IP-телефонією, вважаючи, що рівень безпеки таких мереж є низьким. Сьогодні можна сказати, що IP-телефонія стала певним стандартом телефонного зв'язку. Це пояснюється зручністю, відносною надійністю та відносно низькою вартістю IP-телефонії порівняно з аналоговим зв’язком. Можна стверджувати, що IP-телефонія підвищує ефективність ведення бізнесу та дозволяє виконувати раніше недоступні операції, такі як інтеграція з різними бізнес-додатками.

Якщо ми говоримо про недоліки та недоліки IP-телефонії, то перш за все слід звернути увагу на ті самі «хвороби», які вражають інші служби, що використовують протокол IP. Вони вразливі до атак черв'яків та вірусів, атак DoS, несанкціонованого віддаленого доступу тощо. Хоча ця послуга, як правило, відокремлена від мережевих сегментів, в які "проходять" неголосові дані при побудові інфраструктури IP-телефонії, це не є гарантією безпеки. Сьогодні багато компаній інтегрують IP-телефонію з іншими програмами, такими як

електронна пошта. З одного боку, це створює додаткові зручності, з іншого - і нові прогалини. Більше того, для роботи мережі IP-телефонії потрібна велика кількість компонентів, таких як сервери підтримки, комутатори, маршрутизатори, брандмауери, IP-телефони тощо.

Аналіз літератури свідчить про те, що ринок послуг IP-телефонії в останні роки динамічно розвивався, що робить його дуже привабливим для операторів. Більшість гравців на ринку вважають, що існує тенденція переходу від традиційної телефонії до рішень VoIP. Клієнти віддають перевагу рішенням VoIP, що в основному пов'язано з меншими витратами на зв'язок із збільшенням якості голосу. Значний внесок у розвиток технологій ІВ внесли такі видатні зарубіжні вчені, як І. Бакланов, В. Вишневський, В. Стеклов, А. Суховицький, А. Пінчук, Д. Брау, Д. Ломакін, М. Кульгін, Б. Гольдштейн, Т. Кучникова. т. д.

Було з’ясовано, що стереотип "впровадження корпоративної IP-телефонії в невеликому офісі дорого коштує" зараз застарів хоча б тому, що майже всі існуючі постачальники корпоративної IP-телефонії мають в своєму арсеналі товарні лінії, орієнтовані на цей клас споживачів. Більше того, стартувала уніфікована комунікаційна технологія, корпоративна IP-телефонія якої є основним елементом минулого життя. І що говорить нам про те, що сучасне спілкування - це не спілкування, а те, як ми можемо ефективно вести свій бізнес, не витрачаючи час на непродуктивні затримки. А ефективність потрібна всім - великим і малим. І цінність (не ціна) результативності для будь-якого бізнесу така ж висока.

Встановлено, що вартість експлуатації корпоративної системи IP-телефонії на 40-85% нижча, ніж у традиційної телефонної системи. Закупівельна вартість традиційного обладнання для IP-телефонії приблизно однакова або може відрізнятися на 10-15%. Якщо компанія вже має або розгортає конвергентну IP-інфраструктуру, перехід на корпоративну IP-телефонію буде дешевшим, ніж придбання традиційного телефонного обладнання.

Література:

1. Стеклов В.К., Беркман Л.М. Проектування телекомунікаційних мереж 2010– с. 113-126.

2. Кузнецов А.Е., Пинчук А.В, Суховицкий А.Л. Построение сетей IP- телефони /Компьютерная телефония, 2010, №6. – с. 166-194.

3. Прохоров А. Прогнозы развития информационных технологий // Компьютер Пресс.– 2010. –№1. – с.23-32

АНАЛІЗ ОСОБЛИВОСТЕЙ БЕЗДРОТОВОЇ СЕНСОРНОЇ МЕРЕЖІ ZIGBEE

Волощакевич Владислав Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

ZigBee був створений з потрібні у ряду додатків в певному типі мережі зв'язку, що не володіє високою швидкістю передачі даних, але що є надійним (здатним до самовідтворення), простим в розгортанні і експлуатації. Відмінністю бездротових сенсорних мереж, тобто мереж датчиків від інших типів мереж, є спосіб передачі даних по мережі. Даний принцип дозволяє збирати інформацію з безлічі об'єктів, які за своїми розмірами перевершують радіус зв'язку одного вузла бездротової сенсорної мережі.

Вузли бездротової сенсорної мережі є незалежними, вони можуть містити в собі різну кількість елементів, таких як, датчики для контролю зовнішнього середовища, мікрокомп'ютер і малопотужніого радіо-приймача та радіо-передавача і т.д.

Стандарт ZigBee визначає три типи пристроїв: координатори ZigBee, маршрутизатори ZigBee і кінцеві пристрої ZigBee. Кожна бездротова сенсорна мережа зазвичай містить один координатор [1].

Важливо також, щоб обладнання таких мереж допускало тривалу роботу від автономних джерел живлення, мало низьку вартість, і було компактним.

Особливостями бездротової мережі ZigBee є:

- комірчастої (mesh) топології мережі і алгоритми маршрутизації мережу ZigBee забезпечують самовідновлення і гарантовану доставку пакетів у випадках обриву зв'язку між окремими вузлами (появи перешкоди), перевантаження або відмови якогось елементу;
- передбачається криптографічний захист даних, переданих по бездротових каналах;
- пристрої ZigBee відрізняються низьким електроспоживанням, в особливості кінцеві пристрої, для яких передбачений режим «сну», що дозволяє цим пристроям працювати до трьох років від батарейок AA;
- мережа ZigBee є самоорганізуючою, її структура задається параметрами профілю стека конфігуратора і формується автоматично шляхом приєднання (повторного приєднання) до мережі утворюють її пристроїв, що забезпечує простоту розгортання і легкість масштабування шляхом простого приєднання додаткових пристроїв;
- пристрої ZigBee компактні і мають досить невисоку вартість.

Зв'язок в мережі ZigBee здійснюється шляхом послідовної ретрансляції пакетів від вузла джерела до вузла адресата. У мережі ZigBee передбачено кілька альтернативних алгоритмів маршрутизації, вибір яких відбувається автоматично.

Стандарт передбачає можливість використання каналів в декількох частотних діапазонах. Найбільша швидкість передачі і найкраща стійкість досягаються в діапазоні від 2,4 до 2,48 ГГц.

У цьому діапазоні передбачено 16 каналів по 5 МГц.

На противагу мінімізації енергоспоживання, компактності і дешевизни - відносно низька швидкість передачі даних.

«Брутто» швидкість (включаючи службову інформацію) становить 250 кбіт/с.

Середня швидкість передачі корисних даних, в залежності від завантаження мережі і числа ретрансляції, становить від 5 до 40 кбіт / с.

Відстань між робочими станціями мережі становить десятки метрів всередині приміщень і сотні метрів на відкритому повітрі.

За рахунок ретрансляції покривається мережею зона може бути досить значною: до кількох тисяч квадратних метрів в приміщенні і до декількох гектар на відкритому просторі. Мережа ZigBee в будь-який момент може бути розширена додаванням нових елементів пли навпаки розбита на кілька зон простим призначенням відповідного числа нових конфігуратор мережі. Це буває корисно для зниження навантаження і відповідно підвищення швидкості передачі даних [2].

Література:

1. Пахомов С. Технологии беспроводных сетей семейства 802.15.4 // Компьютер Пресс.-2017.-N5.С.66-81.

2. 802.15.4 IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements. The Institute of Electrical and Electronics Engineers, Inc., New York. – 2016.- 49 - 54 с.

ВІДМІННОСТІ ГЛОБАЛЬНОЇ (WAN) ВІД ЛОКАЛЬНОЇ (LAN) МЕРЕЖІ

Гридяєва Вероніка Русланівна
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Протягом останнього десятиліття дедалі ширший розвиток отримують глобальні обчислювальні й інформаційні мережі – унікальний симбіоз комп'ютерів і комунікацій.

Відбувається активне приєднання всіх країн до всесвітніх мережних структур. Світовою системою комп'ютерних комунікацій щодня користуються більш як 30 млн. людей. Зростає потреба в засобах структурування, накопичення, збереження, пошуку і передачі інформації. Задоволенню цих потреб служать інформаційні мережі та їхні ресурси. Спільне використання ресурсів мереж (бібліотек програм, баз даних, обчислювальних потужностей) забезпечується технологічним комплексом і засобами доступу.

Глобальні мережі відрізняються від локальних тим, що розраховані на необмежене число абонентів і використовують, як правило, не дуже якісні канали зв'язку й порівняно низьку швидкість передачі, а механізм керування обміном, у них в принципі не може бути гарантовано швидким. У глобальних мережах набагато важливіше не якість зв'язку, а сам факт її існування. Правда, зараз вже не можна провести чітку і однозначну межу між локальними та глобальними мережами. Більшість локальних мереж мають вихід в глобальну мережу, але характер переданої інформації, принципи організації обміну, режими доступу, до ресурсів усередині локальної мережі, як правило, сильно відрізняються від тих, що прийнято в глобальній мережі. І хоча всі комп'ютери локальної мережі в даному випадку включені також і в глобальну мережу, специфіку локальної мережі це не скасовує. Можливість виходу в глобальну мережу залишається всього лише одним з ресурсів, поділені користувачами локальної мережі.

Далі розглядаються основні відмінності локальних мереж від глобальних більш детально.

Клас локальних обчислювальних мереж по визначенню відрізняється від класу глобальних мереж невеликою відстанню між вузлами мережі. Це в принципі робить можливим використання в локальних мережах якісних ліній зв'язку: коаксіального кабелю, витої пари, оптичноволоконого кабелю, які не завжди доступні (через економічні обмеження) на великих відстанях, властивих глобальним мережам. У глобальних мережах часто застосовуються вже існуючі лінії зв'язку (телеграфні або телефонні), а в локальних мережах вони прокладаються заново. Складність методів передачі і обладнання. У умовах низької надійності фізичних каналів в глобальних мережах потрібні складніші, ніж в локальних мережах, методи передачі даних і відповідне обладнання. Так, в глобальних мережах широко застосовуються модуляція, асинхронні методи, складні методи контрольного підсумовування, квотування і повторна передача спотворених

кадрів. З іншого боку, якісні лінії зв'язку в локальних мережах дозволили спростити процедури передачі даних за рахунок застосування немодульованих сигналів і відмови від обов'язкового підтвердження отримання пакету.

Швидкість обміну даними. Однією з головних відмінностей локальних мереж від глобальних є наявність високошвидкісних каналів обміну даними між комп'ютерами, швидкість яких (10,16 і 100 Мбіт/с) порівнянна з швидкостями роботи пристроїв і вузлів комп'ютера дисків, внутрішніх шин обміну даними тощо. За рахунок цього у користувача локальної мережі, підключеного до виділеного ресурсу (наприклад, диску сервера), що розділяється, складається враження, що він користується цим диском, як «своїм». Для глобальних мереж типові набагато нижчі швидкості передачі даних 2400, 9600, 28800, 33600 біт/с, 56 і 64 Кбіт/с і тільки на магістральних каналах до 2 Мбіт/с.

Різноманітність послуг. Локальні мережі надають, як правило, широкий набір послуг це різні види послуг файлової служби, послуги друку, послуги баз даних, електронна пошта і інші, в той час як глобальні мережі в основному надають поштові послуги, а іноді файлові послуги з обмеженими можливостями передачі файлів з публічних архівів віддалених серверів без попереднього перегляду їх змісту.

Оперативність виконання запитів. Час проходження пакету через локальну мережу звичайно становить декілька мілісекунд, час же його передачі через глобальну мережу може досягати декількох секунд. Низька швидкість передачі даних в глобальних мережах ускладнює реалізацію служб для режиму on-line, який є звичайним для локальних мереж.

Розділення каналів. У локальних мережах канали зв'язку використовуються, як правило, спільно відразу декількома вузлами мережі, а в глобальних мережах індивідуально.

Використання методу комутації пакетів. Важливою особливістю локальних мереж є нерівномірний розподіл навантаження. Відношення пікового навантаження до середньої може становити 100:1 і навіть вище. Такий трафік звичайно називають пульсуючим. Через цю особливість трафіка в локальних мережах для зв'язку вузлів застосовується метод комутації пакетів, який для пульсуючого трафіка виявляється набагато ефективнішим, ніж традиційний для глобальних мереж метод комутації каналів. Ефективність методу комутації пакетів полягає в тому, що мережа загалом передає в одиницю часу; більше даних своїх абонентів. У глобальних мережах метод комутації пакетів також використовується, але нарівні з ним

часто застосовується і метод комутації каналів, а також некомутовані канали як успадковані технології некомп'ютерних мереж.

Масштабованість. «Класичні» локальні мережі володіють поганою масштабованістю через жорсткість базових топологій, що визначають спосіб підключення станцій і довжину лінії. При використанні багатьох базових топологій характеристики мережі різко погіршуються при досягненні певної межі за кількістю вузлів або протяжністю ліній зв'язку. Глобальним же мережам властива хороша масштабованість, оскільки вони спочатку розроблялися з розрахунку на роботу з довільними топологіями.

Література:

1. https://sites.google.com/site/gxdghxjsruujr/vidminnosti-globalnoie-wan-vid-lokalnoie-lan-merezi

2. https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi

ПЕРЕДУМОВИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ 4G І 5G ЯК СКЛАДОВИХ ІННОВАЦІЙНОГО РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВ УКРАЇНИ

Грушковський Владислав В'ячеславович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Кризові явища у економічному, соціально-політичному та науково-технологічному житті України негативно вплинули на одну з найбільш інноваційних складових народного господарства – телекомунікаційну галузь. Нові технологічні проекти світового співтовариства щодо впровадження на території нашої держави 4G і 5G – допоможуть не лише скоротити зростаючий технологічний відрив, а й стати додатковим імпульсом інноваційної активності телекомунікаційних підприємств.

Питання перспектив формування ринку телекомунікацій на інноваційних засадах, проблем інноваційного розвитку телекомунікаційних підприємств України досліджувалися такими вченими, як - С.О. Гапоненко, М.А. Дем'янчук, Л.А. Захарченко, Я.Т. Карпа, Г.В. Толкачова та іншими.

В цілому процес прийняття управлінських рішень складається з наступних етапів: збір і аналіз інформації; діагностика факторів, що визначають вирішення проблеми; формування альтернативних варіантів вирішення проблеми, вибір і прийняття рішення. При цьому, остаточне рішення залежить як від рівня обґрунтованості, ступеня врахування об'єктивних чинників впливу – зовнішніх на мега та мезорівнях і внутрішніх на мікрорівні (фінансово - економічних,

нормативно - правових, організаційних, технологічний та інформаційних), так і від суб'єктивних чинників на макрорівні, які обумовлюються якісним потенціалом керівного складу (фаховість, досвід, інтуїція і готовність до змін, морально-етичні якості).

Розглянемо основні чинники впровадження 4G і 5G в Україні. До зовнішніх чинників на мега-рівні слід віднести: економічне, політичне, соціальне, техніко-технологічне та науково-технічне середовище розвитку галузі в Україні та її відповідність світовим критеріям. Стосовно до можливостей впровадження 4G і 5G в Україні на мега-рівні визначальну роль грає базовий потенціал інформаційно-телекомунікаційних технологій, досить повна аналітична оцінка якого знайшла відображення у відповідних рейтингах. Всі рейтинги, які відображають стан розвитку галузі, можна розділити на дві групи. До першої слід віднести рейтинги інформаційно-комунікативного розвитку, що характеризують рівень розвитку ІКТ в країнах світу: Індекс розвитку інформаційно-комунікаційних технологій, Індекс мережевої готовності, Індекс інформаційного суспільства, Індекс цифрових можливостей, Індекс можливостей розвитку ІКТ, Індекс дифузії ІКТ, Індекс цифровий доступності, індекс електронної готовності, індекс технологічної готовності, індекс розвитку електронного уряду, індекс цифрового поділу, Міжнародний індекс розвитку Інтернету тощо. До другої групи рейтингів доцільно включити рейтинги науково-технічного розвитку країн, при розрахунку яких використовуються дані по телекомунікаційної галузі або враховується їх безпосередній зв'язок з ІКТ сферою, а саме: Індекс технологічних досягнень, Індекс економіки знань, Глобальний індекс інновацій, Індекс глобальної конкурентоспроможності тощо.

Технологічний прорив телекомунікаційної сфери нашої держави можливий лише за умов активізації інноваційної складової. Таким інструментом для ІКТ підприємств можуть стати технологічні проекти світового співтовариства щодо впровадження 4G і 5G технологій. Однак прийняття відповідних рішень на рівні керівництва підприємств залежить від формування передумов, як зовнішніх на макро та мезо рівнях, так і внутрішніх на макрорівні. І все ж, з огляду на вітчизняний техніко-технологічний потенціал галузі, наявність базової інфраструктури телекомунікацій, зростаючий попит з боку ринку на нові технології, високопрофесійний кадровий потенціал, при наявності державної підтримки та ЄС -

орієнтованої політики держави, впровадження 4G і 5G в Україні - перспектива цілком можлива.

Література:
1. О. В. Виноградова, С. В. Гончаренко // Економіка. Менеджмент. Бізнес

ПЕРЕВАГИ ТА НЕДОЛІКИ ОПТИЧНО-ВОЛОКОННИХ ЛІНІЙ ЗВ'ЯЗКУ

Д'яченко Олексій Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

З кожним днем збільшується попит на високу швидкість передачі данних та збільшення пропускної здатності мереж. Ці фактори утворюють необхідність у розвиненні ліній зв'язку. ВОЛЗ (волоконно - оптичні лінії зв'язку) є найперспективнішим напрямом розвитку, який допоможе вирішити ці питання.

Волоконно-оптичні лінії зв'язку – це вид зв'язку, при якому інформація передається по отптичним діелектричним волокнам. Основна задача – це передача інформації, яка закодована в оптичному сигналі. В загальному вигляді ВОЛЗ містить вхідний кодувальний пристрій (КП), передавач, оптичний кабель, ретранслятор (Р), приймач і декодувальний пристрій (ДКП). Закодована в КП інформація надходить на передавач, що складається з джерела випромінювання (ДВ) і модулятора (М). В якості джерела випромінювання в системах оптичного зв'язку використовують твердотілі і напівпровідникові лазери, а також світлодіоди. Модулятор управляє інтенсивністю випромінювання, що надходить від ДВ. Таким чином, оптичним кабелем розповсюджується змінний оптичний сигнал,що несе закодовану інформацію. При великій довжині ВОЛЗ спостерігається сильне ослаблення світлового променя, тому для відновлення його інтенсивності використовується ретранслятор. В приймачі оптичне випромінювання знову перетворюється в електричний сигнал і посилюється за потужністю з допомогою підсилювача (П). Декодувальний пристрій дозволяє розшифрувати передану інформацію.

Рис.1. Структурна схема волоконно-оптичної лінії зв'язку

Основні переваги ВОЛЗ:

1. Широкий діапазон робочих частот (до 1 ГГЦ), що дозволяє одним оптичним кабелем одночасно передавати до 1010 телефонних розмов або 106 телепрограм.

2. Висока завадостійкість від зовнішніх електромагнітних впливів і міжканальних взаємних наводок, що особливо важливо при високій щільності комунікацій.

3. Малі габаритні розміри і маса через відмову від важких екранувальних оболонок, що дає в бортовій апаратурі виграш у порівнянні з електричним кабелями в 3-5 разів.

4. Таємність інформації , що передається, бо ВОЛЗ практично не дає випромінювання в навколишній простір, а виготовлення відводу призводить до порушення цілісності оптичного кабелю.

5. Потенційно низька вартість внаслідок заміни дорогих кольорових металів (мідь, свинець) матеріалами з необмеженими сировинними ресурсами (скло,кварц,полімери).

6. Довготривалість. Нині термін служби ВОЛЗ складає 25 років.

7. Вибухово-пожежна безпека. Унаслідок відсутності іскроутворення оптичне волокно підвищує безпеку мереж зв'язку при обслуговуванні систем(структур), в яких використовують технологічні процеси з підвищеним ризиком.

Недоліки ВОЛЗ:

1. Вартість інтерфейсного обладнання. Електричні сигнали повинні перетворюватися в оптичні і навпаки. Ціна на оптичні передавачі та приймачі залишається поки що досить високою.

2. Монтаж і обслуговування оптичних ліній. Вартість робіт по монтажу, тестування та підтримки волоконно-оптичних ліній зв'язку також залишається високою.

3. Вимога спеціального захисту волокна. Оптичне волокно має мікротріщини, які ініціюють розрив.

Переваги від застосування волоконно-оптичних ліній зв'язку настільки значні, що не дивлячись на перераховані недоліки оптичного волокна, подальші перспективи розвитку технології ВОЛЗ в інформаційних мережах більш ніж очевидні.

Література:

1. *http://um.co.ua/6/6-12/6-121379.html*
2. *https://www.tls-group.ru/services/inzhenernaya-infrastruktura-zdaniy/strukturirovannye-kabelnye-sistemy/opt-set/*
3. *https://opticstoday.com/katalog-statej/stati-na-ukrainskom/elementi-ta-pristroi-sistem-upravlinnya-avtomatiki/optoelektronni-vimiryuvalni-peretvoryuvachi/volokonno-optichni-linii-*

zvyazku.html#:~:text=%D0%92%20%D0%B7%D0%B0%D0%B3%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%BC%D1%83%20%D0%B2%D0%B8%D0%B3%D0%BB%D1%8F%D0%B4%D1%96%20%D0%B2%D0%BE%D0%BB%D0%BE%D0%BA%D0%BE%D0%BD%D0%BD%D0%BE%2D%D0%BE%D0%BF%D1%82%D0%B8%D1%87%D0%BD%D0%B0,%D0%B2%D0%B8%D0%BF%D1%80%D0%BE%D0%BC%D1%96%D0%BD%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%94%D0%92%20%D1%96%20%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8F%D1%82%D0%BE%D1%80%D0%B0%20%D0%9C.

4. *https://ua-referat.com*

ОСОБЛИВОСТІ МЕРЕЖ НАСТУПНОГО ПОКОЛІННЯ

Дурман Володимир Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Підтримка широкого спектру послуг є однією з основних характеристик NGN (рекомендація від Y.2001). Тому функціональна архітектура NGN повинна включати методи доступу до послуг і вимагати підтримки ресурсів.

Однією з основних функцій NGN є можливість підтримки мультимедійних послуг (абонентські послуги, відеоконференції, потокове передавання тощо). Не слід обмежувати спосіб доступу користувачів до цих служб, типи протоколів, якими вони можуть користуватися, або способи запиту ресурсів для підтримки мультимедійних послуг. Взагалі кажучи, існує кілька серій послуг, таких як абонентська послуга та послуга передачі даних, які відповідно вимагають певної технології.

Впровадження мереж NGN може спростити управління мережею. Це зумовлено двома причинами: по-перше, приватна мережа інтегрована в одну мережу; по-друге, використовується технологія комутації пакетів на основі протоколу IP. У випадку перевантаження в певному напрямку традиційні мережі з комутацією каналів не забезпечують перенаправлення (якщо не реалізована повна реалізація TMN). Основним атрибутом пакетної мережі є динамічна маршрутизація. При правильному встановленні ця властивість може значно покращити загальну продуктивність мережі. Використовуючи комутацію пакетів, ви можете організовувати об’їзні шляхи та у випадку виходу з ладу певних елементів мережі передачі.

Використання NGN спрощує створення корпоративних мереж. Використовуючи класичні методи побудови мережі, компанії потрібно орендувати окремий канал доступу до Інтернету та певну кількість телефонних ліній, які зазвичай надходять від різних операторів. Використовуйте уніфіковану передачу для керування лише одним з'єднанням. Крім того,

створення корпоративної мережі на основі IP-телефонії (VPN) дозволяє компанії використовувати єдиний пул скорочених телефонних номерів. Варто зазначити, що інтелектуальна мережа з комутацією каналів також дозволяє організовувати такі послуги, але вона не отримала широкого застосування через високу вартість та обмеженість функцій.

Мережа NGN дозволяє підтримувати послуги з абсолютно протилежною продуктивністю - від телеметрії до широкосмугового відео. Він може надати користувачеві пропускну здатність та якість обслуговування, яку він замовив.

Використання конвергентної мережі замість кількох виділених мереж може зменшити кількість обслуговуючого персоналу. Кількість різнорідних пристроїв зменшується. Завдяки використанню операційного центру моніторинг мережі може здійснюватися більш ефективно.

Поява мобільних послуг, нових технологій та їх взаємодії збільшило складність механізмів іменування, нумерації та адресації. Завдяки мобільним послугам, переносу мобільних номерів (MNP), немає необхідності в постійному зв'язку між об'єктами (користувачами чи пристроями), що беруть участь у мережевій діяльності, та їх місцезнаходженнями (місцями, які можна знайти). У всіх випадках між партнером по спілкуванню та його місцезнаходженням встановлюється тимчасовий зв'язок. Навіть у випадку фіксованого доступу користувачі та / або пристрої можуть час від часу переміщуватися, залишаючи одне і те ж ім'я чи номер, або присвоюючи нове ім'я чи номер. В останньому випадку попереднє ім'я та номер можуть бути перепризначені іншому користувачеві чи пристрою.

На відміну від NGN, багато існуючих мереж та їх служби вертикально інтегровані, тобто вони не мають чіткого розділення між послугою та передачею пакетів даних. Очевидно, що багатьом службам доведеться працювати над гібридною комбінацією технологій NGN та інших технологій. У цьому випадку необхідно організувати їх взаємодію. Цей процес є дуже складним і включає домовленості між одним або декількома рівнями в архітектурах NGN та non-NGN. Ці питання потрібно розглядати на конкретних прикладах. Деякі аспекти цієї взаємодії описані нижче.

Література:

1. Сети следующего поколения NGN. Под ред. А.В.Рослякова. – М.: Эко-Трендз, 2008. – 424 с.

2. Бакланов И.Г. NGN: Принципы построения и организации. – М.: Эко-Трендз, 2007. – 400 с.

3. Слепов Н.Н. Современные цифровые технологии глобальных сетей связи. – М.: Астра-полиграфия, 2011. – 298 с.

ПЕРСПЕКТИВИ ОПТОВОЛОКОННОГО ІНТЕРНЕТУ

Дурман Володимир Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Серед усіх існуючих методів зв'язку оптичне волокно (діелектричний хвилевід) має найбільшу пропускну здатність. Волоконно-оптичні кабелі використовуються для створення волоконно-оптичних ліній зв'язку, які можуть забезпечити найвищу швидкість передачі даних (залежно від типу використовуваного активного обладнання, швидкість передачі даних може становити десятки гігабіт в секунду або навіть терабайт).

Підключення до Інтернету за допомогою оптичних кабелів може принести клієнтам багато переваг. Через якісні характеристики оптичного волокна подібні канали зв'язку відрізняються:

- міцність і відмінна продуктивність;
- якість та безпека з'єднання бездоганні - майже повністю виключає несанкціоноване втручання в мережу;
- визький рівень шуму, сильна здатність проти перешкод;
- високошвидкісна передача даних, включаючи аудіо- та відеоінформацію;
- відкритість системи використовується для організації додаткових послуг, включаючи телефонну інфраструктуру, мережі відеоспостереження та обладнання безпеки.

Оскільки кабелі не мають обмежень щодо довжини каналу, оптоволоконний Інтернет дозволяє навіть підключатися до віддалених об'єктів.

Якщо ваш домашній Інтернет має максимальну швидкість 10-24 Мбіт/с при завантаженні та максимальну швидкість 1 Мбіт/с при передачі даних, ви все ще використовуєте технологію ADSL. Якщо у вас є технічні можливості і ви хочете «пришвидшити» до 100 Мбіт/с, виправити цю ситуацію легко. Цього достатньо, щоб вказати адресу постачальника, який готовий підключити вашу квартиру до оптичної мережі з архітектурою FTTB.

Сьогодні більшість багатоквартирних будинків в Україні використовують технологію FTTB («Indoor Optics») для підключення до телекомунікаційної мережі. Це означає, що кожен мешканець такого будинку має реальну або потенційну

можливість надсилати та отримувати дані через Інтернет із дивовижною швидкістю до 100 Мбіт/с.

Кількість користувачів ADSL зменшується щодня, тоді як охоплення волоконно-оптичних мереж швидко зростає. Це не дивно, адже технологія FTTB має очевидні переваги.

Оптичні кабелі не піддаються електромагнітним перешкодам і не бояться атмосферного впливу. Сигнал проходить через волоконно-оптичний кабель із стабільною високою швидкістю.

Волоконно-оптичний кабель простягається лише до вимикача, встановленого на даху або підвалі, і тому захищений від механічних ударів. Мідний дріт з витої пари входить в квартиру. Цей спосіб підключення має безперечні переваги.

Пошкоджений кабель Ethernet можна легко виправити, скрутивши мідний сердечник. Однак, якщо оптичний кабель пошкоджений, відновити цілісність оптичної системи можуть лише професіонали за допомогою спеціального зварювального обладнання.

Література:

1. "Волоконно-оптические линии связи" Справочник. под ред. Свечникова - 240 с.

2. Ионов А.Д. Волоконно-оптические линии передачи: учебное пособие / А.Д. Ионов. – Новосибирск: СибГУТИ, 2003. – 152с

СИСТЕМИ ТА ПРИСТРОЇ

Ємельянов Михайло Олегович
Державний університет телекомунікацій,
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі. Ознайомити слухачів з темою комбінаційні логічні пристрої в напрямку комп’ютерна електроніка.

Мета дослідження. Донести інформацію про комбінаційні логічні пристрої:

1. Комбінаційні схеми.
2. Послідовні схеми.
3. Пристрої.

Результати дослідження.

При з’єднані логічних елементів уторуються пристрої, схеми яких називають логічними. Логічні пристрої бувають двох типів: комбінаційні і послідовні. Пам'ять це властивість системи необхідний час зберігати значення сигналів, які характеризують

внутрішній стан цифрового пристрою. Комбінаційні схеми реалізують функції, значення яких у даний момент часу визначаються тільки сукупністю значень вхідних змінних у цей же момент часу і не залежать від попередніх значень вихідних змінних.

Схемною ознакою таких схем є відсутність кіл зворотних зв'язків. Послідовні схеми реалізують логічні функції, значення яких у даний момент часу визначаються сукупністю вхідних змінних у цей же момент часу а також від значення самої функції на попередньому інтервалі. Послідовні пристрої володіють пам'ятю, а тому в разі зміни сигналів на входах для визначення сигналів на виході ПП необхідно знати в якому стані перебував пристрій на попередньому інтервалі.

Роботу цифрових пристроїв прийнято розглядати у безрозмірному дискретному часі. Для цього реальний час розбивається на інтервали, які нумеруються з якого-то моменту. Кожний такий проміжок часу називають тактовим інтервалом або просто тактом. Відновлення інформації на виходах ЦП відбувається на початку нового такту.

Основні типи комбінаційних пристроїв:

- мультиплексори;
- демультиплексори;
- суматори;
- шифратори;
- дешифратори;
- перетворювачі кодів;
- схеми рівнозначності кодів;
- схеми порівняння двійкових чисел;
- порогові схеми;
- мажоритарні елементи та інші.

Мультіплексор - пристрій, що має кілька сигнальних входів, один або більше керуючих входів і один вихід. Мультиплексор дозволяє передавати сигнал з одного із декількох входів на один вихід; при цьому вибір бажаного входу здійснюється подачею відповідної комбінації керуючих сигналів.

Демультиплексор - це логічний пристрій, призначений для перемикання сигналу з одного інформаційного входу на один з інформаційних виходів. Таким чином, демультиплексор в функціональному відношенні протилежний мультиплексору.

Шифратор - логічний пристрій, що виконує логічну функцію перетворення позиційного n-розрядного коду в m-розрядний двійковий, трійчастий або k-ічний код.

Дешифратор - це комбінаційний пристрій, що перетворює кожну вхідну комбінацію двійкового коду в керуючий сигнал лише на одному із своїх виходів. Дешифратор має число n входів і m виходів.

Перетворювачі кодів призначені для перетворення одного паралельного коду в інший. Для подання інформації в цифрових пристроях використовують різноманітні двійкові та двійково-десяткові коди.

Цифрові компаратори виконують порівняння двох чисел, поданих у двійковому або двійково-десятковому коді. В залежності від схемного виконання цифрові компаратори можуть визначати рівність A=B (A і B – незалежні числа з однаковою кількістю розрядів) або нерівності A<B чи A>B.

Результат порівняння відображається відповідним логічним рівнем на виході компаратора. Мікросхеми цифрових компараторів виконують, як правило, усі три операції і мають три виходи.

Суматори це комбінаційні пристрої, призначені для додавання двох чисел представлених у двійковому коді. За характером дії суматори можуть бути комбінаційними і накопичувальні. За способом додавання вони діляться на послідовні і паралельні. Додавання чисел у послідовних суматорах відбувається порозрядно, послідовно в часі.

Висновки та перспективи.

Отже, комбінаційні логічні пристрої – це пристрої, які оброблюють інформацію в цифровій формі. Саме тому вони являються дуже важливим елементом в направленні комп’ютерна електроніка.

Література:

1. *https://sites.google.com/site/naukatatehnologia/komp-uterna-elektronika*
2. *https://ela.kpi.ua/bitstream/123456789/27548/1/Komp_elektronika.pdf*

ЯК ПРАЦЮЄ ПОШУКОВА СИСТЕМА ВЕБ-СЕРВІСІВ ДЛЯ ПОШУКУ ТЕКСТОВОЇ АБО ГРАФІЧНОЇ ІНФОРМАЦІЇ У ВСЕСВІТНІЙ ПАВУТИНІ

Єрошенко Андрій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Пошукова система (англ. Search engine) - алгоритми і реалізує їх сукупність комп'ютерних програм, що надає користувачеві можливість

швидкого доступу до необхідної йому інформації за допомогою пошуку в великої колекції доступних даних. Одне з найбільш відомих застосувань пошукових систем - веб-сервіси для пошуку текстової або графічної інформації у Всесвітній павутині. Існують також системи, здатні шукати файли на FTP-серверах, товари в інтернет-магазинах, інформацію в групах новин Usenet.

Основні складові пошукової системи: пошуковий робот, індексатор, пошуковик.

Як правило, системи працюють поетапно. Спочатку пошуковий робот отримує контент, потім індексатор генерує доступний для пошуку індекс, і нарешті, пошуковик забезпечує функціональність для пошуку індексованих даних. Щоб оновити пошукову систему, цей цикл індексації виконується повторно.

Пошукові системи працюють, зберігаючи інформацію про багатьох веб-сторінках, які вони отримують з HTML-сторінок. Пошуковий робот або «краулер» (англ. Crawler) - програма, яка автоматично проходить по всіх посиланнях, знайденим на сторінці, і виділяє їх. Краулер, грунтуючись на посиланнях або виходячи із заздалегідь заданого списку адрес, здійснює пошук нових документів, ще не відомих пошуковій системі. Власник сайту може виключити певні сторінки за допомогою robots.txt, використовуючи який можна заборонити індексацію файлів, сторінок або каталогів сайту.

Пошукова система аналізує вміст кожної сторінки для подальшого індексування. Слова можуть бути вилучені із заголовків, тексту сторінки або спеціальних полів - метатегов. Індексатор - це модуль, який аналізує сторінку, попередньо розбивши її на частини, застосовуючи власні лексичні та морфологічні алгоритми. Всі елементи веб-сторінки вичленяються і аналізуються окремо. Дані про веб-сторінках зберігаються в індексному базі даних для використання в повторних запитів. Індекс дозволяє швидко знаходити інформацію за запитом користувача.

Ряд пошукових систем, подібних Google, зберігають вихідну сторінку цілком або її частину, так званий кеш, а також різну інформацію про веб-сторінці. Інші системи, подібні системі AltaVista, зберігають кожне слово кожної знайденої сторінки. Використання кешу допомагає прискорити вилучення інформації з уже відвіданих сторінок. Кешовані сторінки завжди містять той текст, який користувач задав в пошуковому запиті. Це може бути корисно в тому випадку, коли веб-сторінка оновилася, тобто вже не містить текст запиту користувача, а сторінка в кеші ще стара. Ця ситуація пов'язана з втратою посилань (англ. Linkrot) і дружнім по відношенню до користувача (юзабіліті) підходом Google. Це передбачає видачу з кешу коротких фрагментів тексту, що містять текст запиту. Діє

принцип найменшого подиву, користувач зазвичай очікує побачити шукані слова в текстах отриманих сторінок (User expectations). Крім того, що використання кешованих сторінок прискорює пошук, сторінки в кеші можуть містити таку інформацію, яка вже ніде більше не буде доступною.

Пошуковик працює з вихідними файлами, отриманими від індексатора. Пошуковик приймає запити користувачів, обробляє їх за допомогою індексу і повертає результати пошуку. Коли користувач вводить запит в пошукову систему (зазвичай за допомогою ключових слів), система перевіряє свій індекс і видає список найбільш підходящих веб-сторінок (відсортованого за якомусь критерію), зазвичай з короткою анотацією, що містить заголовок документа і іноді частини тексту. Пошуковий індекс будується за спеціальною методикою на основі інформації, витягнутої з веб-сторінок. З 2007 року пошуковик Google дозволяє шукати з урахуванням часу створення шуканих документів (виклик меню «Інструменти пошуку» і вказівку тимчасового діапазону).

Більшість пошукових систем підтримує використання в запитах булевих операторів І, АБО, НЕ, що дозволяє уточнити або розширити список шуканих ключових слів. При цьому система буде шукати слова чи фрази точно так, як було введено. У деяких пошукових системах є можливість наближеного пошуку, в цьому випадку користувачі розширюють область пошуку, вказуючи відстань до ключових слів. Є також концептуальний пошук, при якому використовується статистичний аналіз вживання шуканих слів і фраз в текстах веб-сторінок. Ці системи дозволяють складати запити на природній мові. Прикладом такої пошукової системи є сайт ask com.

Корисність пошукової системи залежить від релевантності знайдених нею сторінок. Хоч мільйони веб-сторінок і можуть включати якесь слово або фразу, але одні з них можуть бути більш релевантні, популярні або авторитетні, ніж інші. Більшість пошукових систем використовує методи ранжирування, щоб вивести в початок списку «кращі» результати. Пошукові системи вирішують, які сторінки більш релевантні, і в якому порядку повинні бути показані результати, по-різному. Методи пошуку, як і сам Інтернет з часом змінюються. Так з'явилися два основних типи пошукових систем: системи зумовлених і ієрархічно упорядкованих ключових слів і системи, в яких генерується інвертований індекс на основі аналізу тексту.

Більшість пошукових систем є комерційними підприємствами, які отримують прибуток за рахунок реклами, в

деяких пошукових системах можна купити за окрему плату перші місця у видачі для заданих ключових слів. Ті пошукові системи, які не беруть грошей за порядок видачі результатів, заробляють на контекстній рекламі, при цьому рекламні повідомлення відповідають запиту користувача. Така реклама виводиться на сторінці зі списком результатів пошуку, і пошукові системи заробляють під час кожного кліка користувача на рекламні повідомлення.

Література:

1. Ашманов И. С., Иванов А. А. Продвижение сайта в поисковых системах. — М.: Вильямс, 2007. — 304 с. — ISBN 978-5-8459-1155-1.

2. Байков В.Д. Интернет. Поиск информации. Продвижение сайтов. — СПб.: БХВ-Петербург, 2000. — 288 с. — ISBN 5-8206-0095-9.

3. Колисниченко Д. Н. Поисковые системы и продвижение сайтов в Интернете. — М.: Диалектика, 2007. — 272 с. — ISBN 978-5-8459-1269-5.

4. Ландэ Д. В. Поиск знаний в Internet. — М.: Диалектика, 2005. — 272 с. — ISBN 5-8459-0764-0.

5. Ландэ Д. В., Снарский А. А., Безсуднов И. В. Интернетика: Навигация в сложных сетях: модели и алгоритмы. — М.: Либроком (Editorial URSS), 2009. — 264 с. — ISBN 978-5-397-00497-8.

ОПЕРАЦІЙНА СИСТЕМА LINUX CENTOS

Каграманова Юлія Костянтинівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Що таке linux?

Linux — це операційна система, ядро якої поширюється на безкоштовній основі. Вона складається з ядра системи і набору невеликих програм, що взаємодіють з цим ядром. Само по собі, без програм, ядро абсолютно не виконує ніякої роботи, але на його основі можна зібрати власну версію операційної системи, дистрибутив.

Почав розробляти ядро ще в 1991 році Лінус Торвальдс, студент з Фінляндії. Найперша версія 0.01 була представлена ним 17 вересня 1991 року. Торгова марка linux була зареєстрована розробником, але сама назва обиралося за допомогою голосування. Нинішній символ операційної систем, пінгвін Такс був придуманий особисто Торвальдсом.

Було зібрано ядро, але для нього ще не існувало програм. Замість того, щоб писати програмну обв’язку з нуля, Торвальдс використав програмне забезпечення проекту GNU, розробленого Річардом Столлманом для руху вільного ПЗ. З тих пір linux розширювалася, з'являлися нові дистрибутиви. На базі

цього ядра була побудована навіть операційна система Android, популярність якої оскаржити неможливо.

Хто користується операційною системою linux?

Якщо у вас є пристрій на базі Android, то ви вже відноситеся до користувачів linux. Операційна система, звичайно, інша, але зібрана вона на основі все того ж ядра. Більшість вбудованих систем вашої домашньої побутової техніки теж працює на базі цього ядра, як і ряд портативних ігрових консолей. Операційна система linux часто ставиться на ноутбуки і комп'ютери в якості найпершої. Купівля комп'ютера з встановленим linux'ом — відмінна можливість отримати "Робочу конячку" і заощадити.

В цілому, сьогодні працювати з цією операційною системою може кожен. Головне — підібрати правильний дистрибутив і добре його налаштувати з урахуванням всіх своїх потреб. Під linux вже доступні самі різноманітні ігри, але ультрасучасні комерційні йдуть тільки під останні версії Windows.

Дистрибутиви linux

Щоб почати користуватися linux, досить обрати відповідний вам дистрибутив, встановити і налаштувати його. Але не завжди це просто, тому що дистрибутивів безліч і linux працює по-різному на різному апаратному забезпеченні. Немає єдиного дистрибутива, який задовольнить потреби кожного користувача.

Найбільш оптимальні дистрибутиви для різних цілей:

1) Parrot. Відмінно підійде системним адміністраторам.
2) Fedora. Призначений для користувача варіант, з яким досить просто працювати.
3) Mint. Настільний дистрибутив.
4) Debian. Універсальний дистрибутив як для сервера, так і для домашнього використання.
5) CentOS. Серверний дистрибутив.
6) Snappy Ubuntu Core. Підійде для інтернету речей.

CentOS

Назва CentOS утворено від Community ENTerprise Operating System. Йтиметься про не особливо новий, але, безсумнівно, заслуговуючий на увагу, дистрибутив CentOS. Розроблена дана операційна система на базі Red Hat Enterprise Linux, відрізняється підвищеною стабільністю, може працювати, як на комп'ютерах з 64-бітної архітектурою, так і 32-бітної. Основною відмінністю від Linux є безкоштовність в поширенні.

Почати варто з того, що всі програмні продукти, які розраховані на роботу в середовищі Linux будуть функціонувати і в CentOS. Крім того, в дистрибутиві є набір влаштованих рішень, які зможуть значно спростити життя програмісту або ж адміністратору в роботі на виділеному сервері.

Операційна система розроблена ентузіастами, тим не менш, вона має постійні оновлення. На даний момент остання восьма версія включає повний пакет усіх необхідних нововведень у сфері захисту. Нові версії випускаються раз в два роки, пакет оновлень кожні півроку.

Дуже актуальним зараз вважається питання: «Чи можна вважати, що CentOS - Linux для новачків?» Відповідь негативна. CentOS - це повноцінна операційна система, яка не є спрощеною низькопробною копією. Це самостійний проект, який, тим не менш, має загальний базовий програмний код з творінням Red Hat Enterprise. Відразу потрібно дати одне важливе пояснення. Це не піратська версія, а цілком легальна система. Якщо говорити більш предметно, вся суть полягає в тому, що Red Hat за власним бажанням викладають у відкритий доступ вихідні коди. Природно, що така благодійність не залишилася, непоміченою. Програмісти з усього світу вирішили створити власний проект.

Red Hat Linux - дистрибутив Linux компанії Red Hat. Випускався в період з 1995 по 2003 рік включно. Ранні версії дистрибутива також носили назви Red Hat Software Linux, Red Hat Commercial Linux і Red Hat LiNUX. На основі Red Hat Linux був створений ряд інших дистрибутивів, в тому числі Mandriva і ASPLinux. Остання версія Red Hat Linux була випущена в 2003 році. У 2004 році Red Hat офіційно припинила підтримку Red Hat Linux. Користувачі могли мігрувати або на комерційний Red Hat Enterprise Linux, або на безкоштовний Fedora. Після закінчення офіційної підтримки проект Fedora Legacy деякий час випускав неофіційні оновлення для Red Hat Linux, поки сам Fedora Legacy не був закритий в лютому 2007 року.

Red Hat - це те ж саме, що Linux?

Спочатку Red Hat добилася успіху в підтримці спеціального дистрибутива Linux, який потім отримав назву «Red Hat Linux». Зростання і надійність Red Hat Linux зробили ці два поняття синонімами в умах багатьох людей. З тих самих перших днів рішення і технології Red Hat грунтувалися на цьому успіху і включали майже всі аспекти IT-стека.

Red Hat курує, захищає і підтримує дистрибутив Linux, нині відомий як Red Hat Enterprise Linux, зміна, яка відбулася в 2003 році в результаті злиття з проектом Fedora Linux Project.

Сьогодні Red Hat Enterprise Linux підтримує програмне забезпечення і технології для автоматизації, хмари, контейнерів, проміжного програмного забезпечення, зберігання, розробки додатків, мікросервісов, віртуалізації, управління та багато чого іншого.

Linux грає важливу роль в якості ядра багатьох пропозицій Red Hat. Це далеко не просто операційна система для серверів - Linux є основою сучасного IT-стека.

Пакетні менеджери спрощують використання чужого коду, надаючи цей код у вигляді незалежних модулів - пакетів. Ці пакети підключаються до свого коду за принципом чорних ящиків - це коли ми не знаємо і нам не важливо як все влаштовано всередині цього ящика, але ми знаємо, що він робить. Завдяки такій слабозв'язаній архітектурі з'являється можливість легко оновлювати чужий код або замінювати один пакет іншим зі схожою функціональністю.

Які пакетні менеджери використовувати?

а) Composer - пакетний менеджер для світу PHP. Використовується для завантаження чужого PHP-коду;

б) Bower - пакетний менеджер для фронтенда. Через нього завантажують всі Javascript-бібліотеки;

в) NPM - пакетний менеджер для середовища NodeJS. Використовують для установки Gulp і його плагінів.

Плюси та мінуси CentOS

Насамперед розглянемо процес установки. Все досить-таки просто і не вимагає від користувачів надмірних зусиль. Викачуємо файл на сайті розробників, записуємо на диск, встановлюємо, власне все. Для того щоб виконати всі ці дії навіть програмістом бути не потрібно, достатньо знань рядового користувача.

Також радує те, що на офіційному сайті розробників є безліч корисних порад та інструкцій, які стануть в нагоді всім, хто бажає скористатися програмою. А ось якщо ви любите слухати музику, під час роботи, то тут доведеться проявити трохи винахідливості. Система в принципі не розрахована на формат mp3, але ogg читає. Пов'язано це з патентними правами, але є чудовий вихід з ситуації, що склалася, досить перекодувати файли, і можна насолоджуватися улюбленою музикою.

Ще одне важливе уточнення, яке припаде до смаку багатьом. CentOS передбачає установку графічного інтерфейсу. Для цього є спеціальні метапакети. Додатково у всіх бажаючих буде можливість встановити «Додатки для Офісу» і «Графічні засоби Інтернет».

З недоліків системи, користувачі часто наголошують на тому, що дистрибутив комплектується не завжди свіжими версіями програм, в тому числі ядро Linux теж не завжди нове. Тому дана система не підходить для тих, хто любить щоденні оновлення. Хоча будь-яку систему можна оновити на свій "смак", і цей недолік не буде вважатися таким істотним.

Безпечність системи

Безпека - це не те, що можна просто розгорнути і забути. Безпека повинна бути невід'ємною частиною будь-якого бізнесу і будь-якої стратегії розгортання.

Краща безпека - багаторівнева. Безпека є цілісною. Коли справа доходить до IT-безпеки, операційна система відіграє роль в ширшій історії, яка йде від фізичного обладнання до людей, які мають доступ до цього устаткування, а також до додатків, що розгорнуті на обладнанні. Більш широкий погляд на безпеку також бере до уваги управління ризиками, дотримання нормативних вимог.

Оскільки Linux є модульним, його безпекою легше управляти. Кожна частина, складова операційної системи Linux може піддаватися аудиту, моніторингу та захисту. У Linux є вбудовані інструменти та модулі, такі як SELinux, які допомагають додатково блокувати, відстежувати, повідомляти і усувати проблеми безпеки. У Linux також робляються узгоджені зусилля по відділенню призначеного для користувача простору від простору ядра, а це означає, що процеси, що виконуються по всій системі, не обов'язково доступні користувачам (в залежності від привілеїв ролей), і, аналогічно, призначені для користувача процеси недоступні. до системи в цілому. Це ключова концепція і засіб реалізації таких технологій, як контейнери і віртуалізація, для яких потрібні окремі, розділені і безпечні робочі навантаження і дозволу.

Звичайно, абсолютно безпечною операційної системи не існує, але є кроки, які ви можете зробити - і переваги, які пропонує Linux, - щоб наблизитися до безпеки.

6 основних команд

Ці команди дозволять вам виконувати в оболонці всі ті завдання, які ви зазвичай виконуєте за допомогою графічного інтерфейсу: створення та видалення директорій, написання, редагування та видалення файлів і т. п.

1. **pwd**

Команда pwd (print working directory - висновок робочої директорії) виводить повний шлях до директорії, в якій ви зараз працюєте. Відкриваючи термінал, зазвичай ви потрапляєте в свою домашню директорію. Таким чином, ввівши команду pwd,

ви отримаєте в виведенні / home / (ваше-ім'я-користувача). У запрошенні командного рядка домашня директорія позначена символом «~».

2. **cd**

Команда cd (change directory - «змінити директорію») змінює робочу директорію на ту, ім'я якої ви вказуєте після імені самої команди. Якщо ви введете cd myfolder, вашої робочої Директорією стане myfolder. Це ім'я також відобразиться в запрошенні командного рядка. Але якщо у вашій поточної директорії немає папки з ім'ям myfolder, ви отримаєте повідомлення про помилку.

Якщо після переходу в іншу директорію ви знову виконайте команду pwd, на екран виведеться повний шлях до вашої нової робочої директорії.

3. **ls**

Команда ls (list - «список»), введена без додаткових аргументів, виводить вміст поточної робочої директорії, а саме - список містяться в ній файлів і директорій. Наприклад, якщо запустити команду ls, перебуваючи в myfolder, ми отримаємо імена містяться в цій папці файлів.

Також можна в якості аргументу команди ввести абсолютний шлях до директорії, яку Ви бажаєте подивитися. Наприклад, якщо ви перебуваєте в домашній директорії і запустіть команду ls / boot, оболонка виведе вміст директорії boot, що знаходиться в кореневій (/) директорії. Ваша робоча директорія при цьому не зміниться.

4. **man**

Команда man (manual - «керівництво») відкриває сторінку керівництва по команді, ім'я якої ви вводите в якості аргументу. Цьому посібнику міститься інформація по всіх командах, доступним в Linux. Там ви знайдете відомості про правильне використання команди і різних доступних опціях.

5. **mkdir**

Команда mkdir (make directory - «створити директорію») створює нову директорію з ім'ям, введеним в якості аргументу команди. Перебувати вона буде в нашій поточній директорії. Наприклад, mkdir hello створить директорію hello всередині поточної директорії. Після її створення можна ввести cd hello і перейти в цю нову директорію. У запрошенні командного рядка «~» зміниться на «hello».

6. **rmdir**

Команда rmdir (remove directory - «видалити директорію») видаляє / стирає директорію, вказану як аргумент команди. Якщо ми введемо rmdir hello, ми видалимо раніше створену

директорію hello. Не можна видалити директорію, перебуваючи в ній. Тому за допомогою cd .. ми перейдемо на рівень вище в ієрархії і вже потім видалимо папку hello.

Література:

1. *https://www.centos.org/*
2. *https://uk.wikipedia.org/wiki/CentOS*
3. *https://www.cnews.ru/news/top/2020-12-10_red_hat_pustila_pod_otkos_linuxdistributiv*
4. *https://pingvinus.ru/news/3280*

ІНТЕРНЕТ РЕЧЕЙ: СУТНІСТЬ ТА ОСОБЛИВОСТІ ЗАСТОСУВАННЯ

Касинець Наталія Василівна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Інтернет речей проникає у всі сфери життя і забезпечує роботу багатьох систем: від суто споживацьких (таких як різноманітні побутові сенсори, носима електроніка, розумні будинки тощо) до індустріальних (керування і моніторинг виробничих процесів, розумні енергосистеми, розумні міста, автономні автомобілі тощо). За допомогою “речей” додана вартість збільшуватиметься [1] за рахунок:

– покращення клієнтського досвіду (customer experience);
– зменшення часу, що проходить від задуму продукту до його появи у продажу (time-to-market);
– поліпшення ланцюжків постачання та логістики;
– збільшення продуктивності працівників;
– більш ефективного використання активів (зменшення витрат).

Розвиток інтернету речей стимулює прогрес у багатьох галузях інженерних наук.

Еталонна архітектура IoT.

У компанії Cisco вважають, що в 2020 році буде більше 50 мільярдів пов'язаних об'єктів при населенні 7 мільярдів людей. Сучасна архітектура Інтернету з її TCP / IP-протоколами не можуть впоратися з такого великого мережею, як IoT. Тому виникає необхідність для нової відкритої архітектури, яка може відправляти дані безпеки, якості та класі, надаючи послуги передачі даних (QoSДля подальшого розвитку IoT запропоновано деяка кількість багаторівневих архітектур безпеки[2]. Наприклад - шестирівнева архітектура, заснована на ієрархічній структурі мереж, як показано на Рисунку 1.1

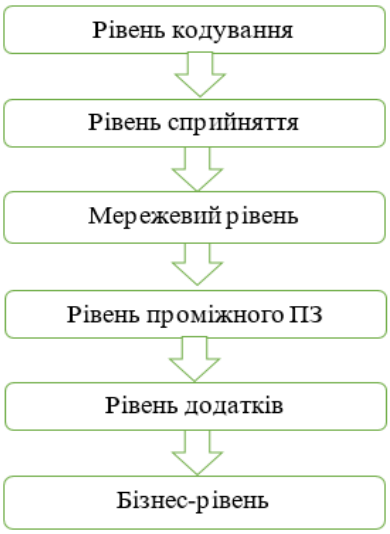


Рисунок 1.1 – Шестирівнева архітектура IoT.

Рівень кодування: ідентифікує об'єкт інтересу (основа Інтернету Речей). Цей рівень призначає кожному об'єкту свій унікальний ідентифікатор (ID), що дозволяє легко розрізняти об'єкти.

***Рівень сприйняття*:** рівень пристроїв IoT, що надає кожному об'єкту фізичне значення. Він складається з датчиків даних різних видів, таких, як RFID-мітки, IR датчики або інші мережі датчиків, які можуть зчитувати температуру об'єкта, вологість, швидкість, місце розташування і т.д. Цей рівень збирає корисну інформацію про об'єктах від датчиків, з'єднаних з ними, і перетворює цю інформацію в цифрові сигнали, які потім передаються на щабель мережі для подальшої обробки.

Мережевий рівень: отримує корисну інформацію в формі цифрових сигналів від рівня сприйняття; та передає її обробляють системам, представленим на рівні проміжного програмного забезпечення через сполучні середовища, такі, як WiFi, Bluetooth, WiMaX, Zigbee, GSM, 3G і т.д., використовуючи протоколи IPv4, IPv6, MQTT, DDS і т.д.

Рівень проміжного програмного забезпечення: обробляє інформацію, отриману від датчиків, використовуючи такі технології, як хмарні обчислення, гарантуючи прямий доступ до бази даних для того, щоб помістити в неї всю необхідну інформацію.

Рівень додатків: реалізує IoT-додатки для всіх видів промисловості на основі оброблених даних. Цей рівень корисний при великомасштабному розвитку мережі IoT. С IoT можуть бути пов'язані розумні будинки, розумні перевезення, розумна планета і т.д.

Бізнес-рівень: управляє програмами та послугами IoT і відповідальний за все дослідження, пов'язані з IoT. Він генерує різні бізнес-моделі для ефективних бізнес рішень.

Типова архітектура Інтернету речей

Архітектура Інтернету речей відрізняється в залежності від реалізації. Один із прикладів архітектури показаний на Рисунку 1.2. Взаємодія з «речами» відбувається через датчики (sensors) та виконавчі механізми (Actuators). Ці датчики разом з усією інфраструктурою для інтеграції з рівнем обробки подій через мережу Internet формують так звану граничну область (**Edge**).

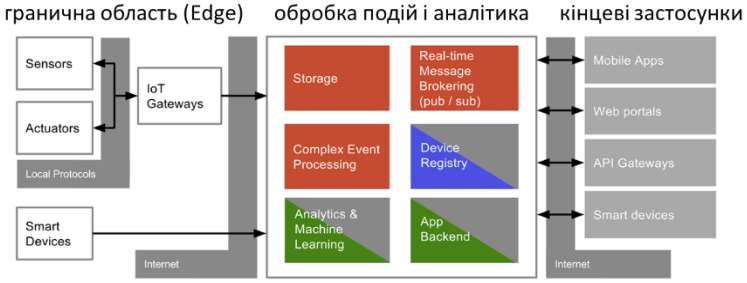


Рисунок 1.2 - Один із прикладів архітектури IoT.

Події (дані), що поступають з граничної області зберігаються і обробляються відповідно до задачі (рівень обробки подій і аналітики, **event processing**, **Platform**). На цьому рівні події (дані) зберігаються, обробляються, перенаправляються потрібним додаткам (Real-Time Message Brokering). Додатково на цьому рівні відбувається адміністрування та керування пристроями з граничної області.

Оскільки ціни на датчики та комунікації продовжують знижуватися, стають рентабельним додавання більшої кількості пристроїв до Інтернет речей. Навіть, якщо в деяких випадках не очевидні переваги.

Розгортання знаходиться на ранній стадії. Більшість компаній, які займаються Інтернетом речей, зараз знаходяться на стадії оцінювання. Причина цього в тому, що необхідні подальші технології – сенсорні технології, 5G і машинознавчі аналітики – все ще знаходяться на досить ранній стадії розвитку. Але кількість підключених пристроїв продовжує зростати, наше життєве та робоче середовище наповнюватиметься розумними продуктами.

Література:

1. *Refactoring: Improving the Design of Existing Code / [Martin Fowler, Kent Beck, John Brant et al.]. – Addison-Wesley Professional, 1999. – 464 p. дата звернення 01.03.2020).*

2. *Evans D. Internet of Things. Cisco, white paper. [Електронний ресурс]: [Інтернет-сайт]. – Режим доступа: https://www.cisco.com/c/dam/en_us/about/ac79/docs/i*

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ ХМАРНИХ СЕРВІСІВ ПРИ ПОБУДОВІ ПЛАТФОРМИ ІНТЕРНЕТУ РЕЧЕЙ

Касинець Наталія Василівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Хмарні технології та Інтернет речей є найбільш перспективними напрямками в інформаційно-комунікаційних технологіях. Інтернет речей (IoT) дозволяє нам з'єднувати людей і пристрої абсолютно новим способом: з'єднанням між фізичними пристроями та віртуальними програмами, дозволяючи передачу даних з реального світу у віртуальний. [1] Ця технологія цікава як для простих приватних користувачів, так і для великих бізнес клієнтів, починаючи від здоров'я та покращення навчання, до промислового виробництв та логістики. [2]

По мірі того, як Інтернет речей (IoT) набув популярності, сучасні хмарні постачальники послуг почали пропонувати сервіси для IoT. З появою мобільних мереж високої продуктивності (LTE 4G, 3G, IEEE 802.11ac, WiFi) з'являється парадигма хмарних обчислень як оптимальне рішення для аутсорсингових обчислень та зберігання даних і виходить за межі обмежень мобільних пристроїв. Завдяки хмарному аутсорсингу та надійному бездротовому підключенню, мобільні пристрої стають інтерфейсами будь-де та будь-коли.

Розробка рекомендацій щодо використання хмарних сервісів

Часто майже кожен розробник або бізнес-клієнт намагається обрати постачальника хмарних сервісів та через поповненя ринку хмарних послуг це зробити з кожним днем все складніше. Тому цей розділ був присвячений розбору хмарних провайдерів, іх сервісів, і розробці рекомендацій.

Складність вибору постачальника хмарного сервісу полягає в тому, що під різні бізнес потреби потрібні різні потужності сервісів, а найбільшою проблемою є те, що не кожен провайдер може позмагатися за довіру клієнта. Тому перейдемо до рекомендацій вибору хмарного IaaS-постачальника.

Рекомендації для вибору хмарного IaaS-постачальника

Зазвичай тип сервісу IaaS (Інфраструктура як послуга) обирають більш досвідчені робітники, але й не розробники, до прикладу: системні адміністратори. Інфраструктура як послуга по своїм об'єктам і характеристикам найбільш наближена до володіння власним "залізом" і віртуалізацією. При виборі IaaS маємо змогу отримати в своє розпорядження хмарні процеси, пам'ять, диски, мережі. Весь цей набір допоможе створити віртуальні сервери-маршрутизатори і налаштувати мережеву топологію так, як це буде необхідно. Обираючи провайдерів хмарних послуг, безумовно, варто відштовхуватися від завдань, які необхідно вирішити, і вимог до надійності сервісів. Наприклад, компаніям зі штатом 5-10 чоловік, вся IT-інфраструктура яких становить сервер бухгалтерії і файловий, в переважній більшості випадків немає необхідності обирати сервіси з найкращою відмовостійкостю. Якщо ж компанія має більший штат та більш істотні запити в IT-інфраструктурі, тоді можна розглядати більш надійних постачальників IaaS, з більшою відвомостійскістью. Безумовною перевагою таких провайдерів є їх близькість до «наземним» інфраструктур з архітектурної точки зору (при переході в хмару зміни в архітектурі сервісів будуть мінімальні).

Ключові параметри, на які потрібно звернути увагу при виборі:

1) ***Лояльність провайдера хмарного IaaS і масштаби клієнта.***

Кожний бізнес чи клієнт, коли починає споживати хмарні рішення перш за все обирає постачальника і створює партнерські відносини. І від якості цих послуг завжди залежить розвиток проекту чи то компанії. Для хмарного провайдера це є основним, адже її досягнення автоматично означає, що замовник продовжить споживати послугу. Певною мірою описану поведінку можна спостерігати у будь-якого сервісного IaaS провайдера, різниця лише в масштабах замовника. На замовників, з якими активно вибудовують відносини українські провайдери хмарних послуг, закордонні - навіть не подивляться.

2) ***Гнучкість провайдера.***

Цей параметр часто виходить з першого. Але зайва гнучкість є поганим сигналом, тому тут треба бути обережним. Що можна розуміти під гнучкістью? Це відбувається тоді, коли провайдер може надати послугу, якої немає ні в каталозі, ні взагалі наявною. Це доволі приємно коли за проханням, для тебе створюють нові функції чи продукти, але це може бути одним з перших критеріїв настороження. Це може означати або те, що продукт зовсім не той яким його описує постачальник, або він

взагалі не готовий. Той провайдер, що задовольняє всі запити клієнтів може в кінці кінців стати досить нестабільним. І це впливає на стабільність надання сервісу;

3) ***Надання тестового періоду.***

Один із важливих аспектів, оскільки за цей період клієнт може зрозуміти чи підходить йому сервіс, чи влаштовує технологічне налаштування і зв'язок зі службою технічної підтримки. За цей період можна оцінити якість сервісу перед запуском;

4) ***Надійність провайдера.***

Надійним буде той провайдер, у якого сервіс буде розділений на декількох географічно-розділених і розміщених майданчиках.

5) ***Похвилинна тарифікація.***

На цей критерій безумовно потрібно звернути увагу, оскільки сервери у провайдера працюють кожну секунду кожного дня, від чого і будуть залежати простої;

6) ***Надійність дата-центра***.

Від надійності Дата-Центру залежить надійність хмарного сервісу;

7) ***Електроживлення та охолодження***.

Кількість ліній постачальників електроенергії, наявність дизель-генераторів і достатність їх для електроживлення Дата-центру в різних умовах;

8) ***Мережева зв'язність.***

Тут важливо звернути увагу не тільки на те, скільки резервних каналів є у провайдера, але і яким чином вони «фізично» прокладені. Адже навіть 3 резервних канали можуть бути відключені одночасно, якщо вони прокладені через одні й ті ж комунікаційні колодязі.

9) ***Фізична безпека***.

Організація фізичної безпеки є важливим фактором, тут варто звернути увагу на самих охоронців (ми не вважаємо, що пари сторожів досить для захисту даних замовників), а також на саму пропускну процедуру і на те, як вона дотримується.

10) ***Юридичні чинники***.

Варто звернути увагу на юридичну прозорість компанії. Правова держава у нас тільки будується, але все ж провайдер, який діє виключно в правовому полі, має більш низькі шанси піддатися переслідуванням з боку зацікавлених сторін, а значить, з великою ймовірністю зможе надавати вам сервіс протягом довгого часу;

11) ***Розташування дата-центру***.

Питання розташування є занадто індивідуальним для того,

щоб можна було дати якусь конкретну рекомендацію. Для деяких замовників важлива мінімальний пінг для адекватної роботи їх інформаційних систем, для інших важлива географічна віддаленість без прив'язки до пінг. Все дуже індивідуально;

12) ***Апаратне забезпечення хмарної платформи***: сучасні хмари мають тонкий баланс між вибором виробника устаткування і використовуваної конфігурації серверів, який дозволяє забезпечити необхідну продуктивність / надійність з одного боку, і прийнятну ціну з іншого.

Рекомендації для вибору хмарного SaaS-постачальника

Даний вид хмарного сервісу зазвичай передбачає надання готового рішення для клієнта з мінімальною необхідність налаштування. Цим сервісом вже можуть керувати не тільки досвідчені адміністратори, але вже й простий користувач з мінімальним залученням адміністратора.

Ключові параметри на які потрібно звернути увагу при виборі:

1) Справжність сервісу.

Сучасні постачальники SaaS не рідко можуть поєднувати локальні системи, розмістити їх в хмарі, а після цього забезпечити користувача потрібним інтерфейсом. Такий сервіс завдасть чимало витрат при модернізації рішень, тому важливо в першу чергу познайомитися з постачальником і провести аналіз чи розроблений сервіс на єдиній базі;

2) Розвиток рішень і продуктів постачальника.

Провайдери SaaS зазвичай випускають оновлення дуже часто, у клієнта же реальна можливість впливати на продукт є тільки в тому випадку, якщо постачальник це дозволить. Переконайтеся, що рішення розвивається в партнерстві з клієнтами і що вам зрозуміло, як саме ви зможете впливати на продукт;

3) ***Технічна підтримка і доставка оновлень***.

Обираючи корпоративну систему SaaS, потрібен партнер, який допоможе використовувати нововведення для підвищення ефективності роботи організації. Необхідно чітко розуміти процеси підтримки продукту, оскільки можливі підводні камені. З'ясуйте, як саме постачальник забезпечує регулярну доставку оновлень; чи є у нього в штаті експерти, здатні допомогти спланувати наступні стадії вашої стратегії і чи зможе він сам або його партнери надавати вам сприяння в довгостроковій перспективі;

4) ***Розкриття.***

Компанії повинні розкривати дані замовників тільки в разі, якщо це потрібно самими замовниками або законом, і повинні при цьому попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів в тій мірі, наскільки це дозволяє законодавство;

5) ***Мережева зв'язність.***

Тут важливо звернути увагу не тільки на те, скільки резервних каналів є у провайдера, але і яким чином вони «фізично» прокладені. Адже навіть 3 резервних канали можуть бути відключені одночасно, якщо вони прокладені через одні й ті ж комунікаційні колодязі.

Рекомендації для вибору хмарного PaaS-постачальника

Існуючі сьогодні PaaS-рішення настільки різноманітні за характером вирішуваних завдань, що виділити їх родову властивість досить важко. Якщо говорити в цілому, то все PaaS-рішення дозволяють підвищити ефективність праці розробників додатків. Однак існує цілий ряд різних підходів та інструментів для вирішення цього завдання. Дійсно, будь-яка PaaS-платформа дозволяє створити динамічний веб-сайт, але кожне окремо взяте PaaS-рішення при цьому надає специфічні можливості і зручності.. Послуги типу PaaS розраховані в першу чергу на розробників. Вони представляють набори готових компонентів для створення додатків, а також фреймворки для управління платформою. В даному випадку компонентами будуть сервіси баз даних, репозиторії, інструменти автоматизованого деплоя, середовища тестування і тому подібні сервіси.

Ключові параметри на які потрібно звернути увагу при виборі:

1) ***Ціна.***

В цьому критерії достатньо знайти відповіді на такі питання «За якою моделлю здійснюється оплата за використання сервісу (за фактом обсягу використаних ресурсів / фіксовані ний пакет)?», «Чи існує безкоштовний ознайомчий варіант?»;

2) ***Підтримувані технології.***

В цьому параметрі потрібно задати такі питання і знайти на них відповідь: «Чи підтримує PaaS-постачальник мови програмування, системи зберігання даних і інфраструктурні сервіси, котрі потрібні зараз і можуть знадобитися в майбутньому?»;

3) ***Можливі інтеграції.***

Цей параметр має на увазі стандартний набір доступних

інструментів, тому потрібно проаналізувати обраний сервіс за таким питаннями: «Чи надаються механізми інтеграції з мобільними платформами, з хмарними системами і інтерфейсами сторонніх постачальників?» «Чи підтримуються стандартні інтерфейси обміну інформацією (REST, JSON)?»;

4) ***Надійність, репутація.***

Є досить багато провайдерів які почали свій шлях вже давно і мають великий набір сервісів, з яких можна обрати щось потрібне дня компанії чи бізнесу. А є й такі, що почали досить недавно і при тому не мають готових сервісів, а тільки розробки. Тож при виборі потрібно розглянути такі питання: «Наскільки давно постачальник присутній на ринку?», «Чи відбувалися збої в роботі постачальника і наскільки оперативно вони усувалися?», «Чи підтримує постачальник можливість розподіленого розміщення додатків і даних одночасно в декількох дата-центрах?»;

5) ***Додаткові сервіси***.

В цьому пункті потрібно звернути увагу на такі питання: «Чи надає постачальник додаткові кошти розробки?», «Які умови технічної підтримки?», «Чи існує каталог додаткових модулів, що дозволяють розширити базову функціональність?», «Чи є у продукту активно підтримуваний форум, вікі сайти і блоги?».

Дослідник з Salesforce.com Джей-Пі Рангасвамі (JP Rangaswami) запропонував набір з «десяти керівних принципів» для хмарних обчислень:

- ***прозорість:*** компанії повинні розкривати внутрішні правила обробки інформації, а також відомості про продуктивність і надійності на публічних веб-сайтах;
- ***обмеження за сферами використання***: компанії не повинні претендувати на володіння даними замовників і можуть використовувати їх тільки в тих цілях, для яких вони були отримані від замовників;
- ***розкриття:*** компанії повинні розкривати дані замовників тільки в разі, якщо це потрібно самими замовниками або законом, і повинні при цьому попередньо повідомляти замовників про розкриття даних на вимогу правоохоронних органів в тій мірі, наскільки це дозволяє законодавство.
- ***система управління безпекою***: компанії повинні мати у своєму розпорядженні потужною системою захисту даних, що відповідає міжнародним стандартам (таким як ISO 27002);
- ***додаткові можливості в сфері безпеки:*** компанії повинні пропонувати замовникам додаткові можливості щодо захисту їх даних;

- ***розташування даних:*** компанії повинні пред'являти замовникам список країн, в яких розміщуються пов'язані з ним дані;

- ***повідомлення про витоки:*** компанії повинні оперативно повідомляти замовників про всі відомі витоках, які ставлять під загрозу конфіденційність або цілісність даних;

- ***аудит:*** компанії повинні звертатися до послуг сторонніх аудиторів з метою перевірки того, наскільки їх система управління безпеки відповідає справжнім вимогам;

- ***переносимість даних:*** компанії повинні надавати замовникам можливість вивантаження даних в стандартному форматі, придатному для передачі через інтернет;

- ***звітність:*** компанії повинні співпрацювати з замовниками в адекватному розподілі обов'язків при складанні звітності про приватності і безпеки [3].

Отже, при використанні хмарних обчислень, споживачі інформаційних технологій можуть істотно знизити капітальні витрати — на побудову центрів обробки даних, закупівлю серверного та мережевого обладнання, апаратних і програмних рішень, щодо забезпечення безперервності і працездатності — так як ці витрати поглинаються провайдером хмарних послуг

Недоліки «хмарних» рішень зводяться, в основному, до проблеми довіри постачальнику сервісу, від якого залежить як безперебійна робота, так і збереження важливих даних користувача. Крім того «хмарні обчислення» висувають високі вимоги до якості каналів зв'язку, які гарантують повсюдний якісний доступ в інтернет.

Література:

1. Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. "Future internet: the internet of things architecture, possible applications and key challenges". In: Frontiers of Information Technology (FIT), 2012 10th International Conference on. IEEE. 2012, pp. 257–260 (дата звернення 10.02.2021).

2. Luigi Atzori, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey". In: Computer networks 54.15 (2010), pp. 2787–2805. (дата звернення 10.02.2021).

3. Облачные сервисы. Взгляд из России. Под ред. Е. Гребнева. — М.: CNews, 2011. — 282 с.(дата звернення 10.02.2021)

КЛАСИФІКАЦІЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Кірюшин Владислав Олексыйович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Телекомунікаційні системи та мережі поділяють за призначенням, принципами побудови, приналежністю тощо.

Транспортна мережа, *або* ядро мережі *(backbone або core network),* — це універсальна мережа, що реалізує функції транспортування/комутації й об’єднує окремі мережі доступу із забезпеченням транзиту трафіка між ними високошвидкісними каналами.

До складу транспортної мережі можуть входити:

- ранзитні вузли, що виконують функції перенесення і комутації;
- кінцеві (граничні) вузли, що забезпечують доступ абонентів до транспортної мережі;
- сервери сигналізації, що виконують функції обробки інформації сигналізації, управління викликами та з’єднаннями;
- шлюзи, що дозволяють здійснити підключення різнорідних, тобто апаратно і програмно несумісних між собою мереж зв’язку.

За територіальним принципом мережі поділяються на:

- глобальні мережі (Wide Area Network, WAN) - розташовується в межах будинків;
- міські мережі (Metropolitan Area Network, MAN) – об’єднання мереж в місті в одну велику мережу;
- локальні мережі (Local Area Network, LAN) - для глобального інтернету наприклад який небуть регіон (країна чи континент)
- Internet – індивідуальний комп’ютер надає доступ до публічної мережі.
- віртуальна приватна мережа (Virtual Private Network, VPN) — індивідуальні комп'ютери під'єднані до інших мереж через сегмент публічної мережі.

За видами комутації мережі поділяють на:

- некомутовані;
- комутовані — з комутацією каналів, повідомлень, пакетів.

За адміністративним розподілом мережі поділяють на:

- магістральну мережу, яка зв’язує між собою телекомунікаційні вузли країни в цілому й забезпечує транзит потоків повідомлень між зоновими мережами;
- зонові (або регіональні) мережі, побудовані в межах території одного або декількох регіонів (груп областей) країни;
- місцеві мережі, які утворені в межах адміністративної або визначеної за іншим принципом території і не належать до регіональних мереж зв’язку. Місцеві мережі поділяються на міські та сільські.

За швидкістю мережі:

- низькошвидкісна (швидкості від кбіт/с до Мбіт/с);

- високошвидкісна (швидкості від сотень Мбіт/с до Гбіт/с).

За типом абонентських терміналів, які використовуються в ТКС, телекомунікаційні мережі поділяються на:

- мережі фіксованого зв'язку, що забезпечують приєднання стаціонарних абонентських терміналів;
- мережі рухомого зв'язку, що забезпечують приєднання рухомих (що перевозяться або переносяться) абонентських терміналів.

За відомчою приналежністю телекомунікаційні мережі поділяють на такі групи:

- мережі зв'язку загального користування;
- виділені мережі зв'язку;
- технологічні мережі зв'язку;
- мережі спеціального призначення.

Мережі кампусів отримали свою назву від англійського слова campus — студентське містечко. Нині цю назву не пов'язують із студентськими містечками, а використовують для позначення мереж підприємств і організацій. Мережі кампусів об'єднують безліч мереж різних відділів одного підприємства в межах окремої будівлі або однієї території, що покриває площу в декілька квадратних кілометрів. Служби такої мережі включають взаємодію між мережами відділів, доступ до загальних баз даних підприємства, факс-серверів, високошвидкісних модемів і високошвидкісних принтерів. У результаті співробітники кожного відділу підприємства дістають доступ до деяких файлів і ресурсів мереж інших відділів. Мережі кампусів забезпечують доступ до корпоративних баз даних незалежно від того, на яких типах комп'ютерів вони розташовуються.

Широкомовна мережа уникає складних процедур маршрутизації (раутінгу), властивих комутованим мережам, приймаючи, що передавання кожного вузла може бути прийняте всіма іншими вузлами в мережі. Іншими словами, широкомовна мережа має тільки один комунікаційний канал. Наприклад, кабельні локальні комп'ютерні мережі є широкомовними мережами, де кожен користувач сполучений з будь-яким іншим і мережа має топологію шини, зірки або кільця. Безпровідні локальні мережі використовують радіо- або оптичні хвилі. Багато сателітарних радіосистем також є широкомовними, оскільки наземна станція в системі може приймати всі повідомлення, які ретранслює сателіт.

Література:
1. https://www.znanius.com/3561.html

2. https://uk.wikipedia.org/wiki/Телекомунікаційна_мережа

РОЗРОБКА ПРОЕКТУ БЕЗДРОТОВОЇ СИСТЕМИ ЗАХИСТУ ТА КОНТРОЛЮ ДОСТУПУ В ПРИМІЩЕННЯ

Ковальчук Євгеній Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Постановка задачі. Задача забезпечення протидії проникнення в приміщення є багатофункціональною та складною. Тому вибір датчиків та схеми їх взаємодії потребує досконального вивчення та дослідження. Цьому присвячена дана робота.

Мета дослідження – вивчення та дослідження побудови оптимальної структури елементів захисту приміщення від проникнення посторонніх осіб.

Досвід впровадження та експлуатації систем GPS-моніторингу транспорту на підприємствах різних галузей показує, що використання GPS трекерів дозволяє максимально ефективно запобігати нецільовому використанню автотранспорту працівниками організації. Таким чином, доцільно дослідити та реалізувати методику застосування GPS трекерів для автотранспортного підприємства. Виконуючі поставлені завдання в дипломній роботі проаналізовано особливості функціонування системи глобального позиціонування та системи GPS-моніторингу транспорту. Виконано дослідження системи супутникових навігаційних систем та дослідження ринку GPS трекерів. У практичній частині обґрунтовано фінансову ефективність застосування GPS трекерів для автотранспортного підприємства

Результати дослідження – в результаті досліджень сформована оптимальна структура периферійного обладнання для запобігання проникнення сторонніх осіб в приміщення.

Висновки і перспективи. Запропонований спосіб є ефективним для захисту приміщень від сторонніх осіб та може бути використаним на практиці.

Література:

1. *https://www.videorus.ru/articles/35/*

РОЗРОБКА МЕТОДИКИ ЗАСТОСУВАННЯ GPS– ТРЕКЕРІВ ДЛЯ АВТОТРАНСПОРТУ «УКРПОШТА»

Корчемська Наталія Олександріна

Об`єкт дослідження – процес впровадження системи контролю за автотранспортом.

Предмет дослідження – система глобального позиціонування та система GPS-моніторингу транспорту.

Мета роботи – дослідження методики застосування GPS–трекерів для автотранспортного підприємства.

Методи дослідження – в дипломній роботі використаний аналіз, порівняння, класифікація, структурно-функціональний метод та прогнозування. Досвід впровадження та експлуатації систем GPS-моніторингу транспорту на підприємствах різних галузей показує, що використання GPS – трекерів дозволяє максимально ефективно запобігати нецільовому використанню автотранспорту працівниками організації. Таким чином, доцільно дослідити та реалізувати методику застосування GPS–трекерів для автотранспортного підприємства.

Виконуючі поставлені завдання в дипломній роботі проаналізовано особливості функціонування системи глобального позиціонування та системи GPS-моніторингу транспорту. Виконано дослідження системи супутникових навігаційних систем та дослідження ринку GPS – трекерів. У практичній частині обґрунтовано фінансову ефективність застосування GPS – трекерів для автотранспортного підприємства.

ВИСНОВКИ

Проаналізувавши актуальність питання впровадженя GPS – трекерів на сьогоднішній день стає зрозуміло що питання контролю є напрочуд гострим питанням для кожної організації, яка хоча б мінімально пов’язана з використанням автотранспорту. Тим паче дане питання є особливо актуальним і можна навіть сказати критичним для автотранспортних підприємств. Стан дослідження питання на сьогоднішній день, можна сказати залишає підгрунтя для розвитку перспективного напрямку, як з наукової так і з практичної точки зору.

В дипломній роботі за допомогою аналізу, порівняння та класифікації досліджненно ринок GPS – трекерів, принципи їх функціонування та розглянута класифікація, актуальних на сьогоднішній день моделей, які є найбільш ефективними та популярними у використанні, як апаратних так і програмних трекерів. За допомогою структурно-функціонального методу досліджено систему глобального позиціонування та супутникові навігаційні системи, що дає теоретичні можливості для

практичної реалізації нових продуктів, які зможуть бути більш ефективними та встигати за розвитком науково-технічного прогресу. За допомогою методів аналізу та прогнозування оцінена та розроблена методика застосування GPS – трекерів для автотранспортного підприємтсва та обгрунтована економічна ефективність її впровадження.

Дослідивши в комплексі всі завдання поставлені на початку дипломної роботи, стає зрозумілим той факт, що питання впровадження та експлуатації GPS трекерів фактично не вимагає значних капіталовкладень на початковому етапі їх закупки та монтажу, враховуючи ту кількість різноманітних варіантів, які доступні на сьогоднішній день на ринку.

В результаті дослідження становлено, що всі витрати підприємства будуть компенсовані вже після першого або максимум другого місяця використання GPS – трекерів. В подальшому ми отримуємо прибутки для підприємства, фактично 66 без додаткових витрат фінансового чи людського ресурсів. Дане питання постає особливо актуальниим враховуючи світові тенденції до мінімізації витрат та оптимізації розподілення коштів в середині бізнес-середовища на період пандемії.

Література:

1. Серапинас Б.Б. Глобальные системы позиционирования. — М. : ИКФ "Каталог", 2012. — 106 с.

2. Соловьев Ю.А. Системы спутниковой навигации.-М. Эко-Трендз, 2009.с

ТЕНДЕНЦІЇ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНОЇ ГАЛУЗІ В 2021 РОЦІ

Костюк Каріна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Телекомунікаційна галузь продовжує невпинно розвиватись, охоплюючи все нові і нові технології, які впевнено продовжують проникати на ринок. Останнім часом у даній галузі відбувається багато змін та впровадження різних новітніх технологій. У 2021 році прийняття останніх галузевих тенденцій, таких як 5G, AI / ML та IoT, зросте і сформує майбутнє телекомунікаційної галузі. Систематичне поєднання операційних та технологічних змін допоможе забезпечити чудову залученість споживачів у телекомунікаційній галузі.

Зробимо короткий огляд технологій, які зараз зростають стрімко і відповідно, ймовірно, матимуть значний вплив на розвиток телекомунікаційної сфери у 2021 році.

Штучний інтелект та машинне навчання (AI / ML) є однією з найважливіших тенденцій телекомунікаційних технологій станом на 2021 рік. За даними Forbes,

«телекомунікації є однією з найбільш швидкозростаючих галузей, яка використовує AI / ML у багатьох аспектах свого бізнесу, від покращення досвіду клієнтів до прогнозного обслуговування до вдосконалення надійності мережі». Інструменти, підпорядковані ШІ, такі як чат-боти та віртуальні помічники, можуть бути використані для забезпечення безперебійної роботи служб підтримки клієнтів. Саме ці інструменти допомагають надавати персоналізовані послуги із залучення клієнтів на основі історії клієнтів.

5G - 5-е покоління, нарешті переходить від стадії ажіотажу до реальності, оскільки деякі провідні телекомунікаційні компанії вже випустили свої комерційні можливості 5G. В даний час телекомунікаційні компанії у всьому світі перебувають на стадії розробки мереж 5G з очікуванням збільшення впровадження 5G у 2021 році. 5G значно прискорить інновації та модернізує різні сектори по всьому світу. Однак це також спричинить нові виклики безпеці для телекомунікаційної екосистеми, з якою потрібно буде працювати по-новому.

Інтелектуальна автоматизація. Найбільшими проблемами, які обтяжують телекомунікаційну галузь сьогодні є конкуренція та постійно зростаючий попит на безперебійне підключення. Але за допомогою цієї інтелектуальної телекомунікаційної технології компанії можуть спростити обробку оперативних завдань. Інтелектуальна автоматизація - це технологія, яка дозволяє автоматизувати бізнес-процес шляхом налаштування програмних роботів або ботів. Вони не тільки скорочують термін очікування, характерний для традиційних засобів обслуговування споживачів, але також забезпечують значне скорочення витрат та безкомпромісний досвід клієнтів.

Інтернет речей (IoT). Оскільки телекомунікаційна індустрія забезпечує підключення до Інтернет-пристроїв, вона має одну з найважливіших ролей на ринку Інтернету речей, повсякденних предметів, які пов’язані між собою та Інтернетом. Оскільки технологія IoT призводить до збільшення кількості пристроїв у мережі, існує більше можливостей для порушення безпеки та конфіденційності, тому телекомунікаційні мережі повинні планувати та готувати захист для цього.

Література:

1. https://dev.to/naveenc65628676/telecom-industry-trends-2021-3kel (дата звернення: 12.02.2020)

2. https://www.bernardmarr.com/default.asp?contentID=1964 (дата звернення: 12.02.2020)

Костюк Каріна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

5G, Інтернет речей, хмарні обчислення та штучний інтелект це саме ті аспекти, які кардинально змінюють телекомунікаційний ландшафт в наш час, в епоху прогресивного оцифрування та високошвидкісного технологічного розвитку. Тому тема симбіозу між штучним інтелектом та телекомунікаціями є досить актуальною на сьогоднішній день. Впровадження ШІ телекомунікаційними компаніями сприяє вдосконаленню процесів управління мережею та надає змогу операторам телекомунікацій надавати своїм клієнтам значно привабливіші послуги, а також покращувати утримання клієнтів.

Головними чинниками зростання штучного інтелекту у телекомунікаційній сфері є постійне збільшення попиту на мережеві рішення з автономним керуванням. Мережі телекомунікаційної галузі швидко розширюються, стаючи ще більш складнішими в управлінні. Використовуючи мережеві рішення, що працюють на основі штучного інтелекту, CSP (постачальники послуг криптографії) можуть зменшити перевантаження мережі та покращити якість мережі, а отже, підвищити взаємодію з клієнтами.

Штучний інтелект можна розділити на різні технологічні сегменти, такі як машинне навчання, глибоке навчання, обробка природної мови, обробка зображень та розпізнавання мови. Однак центральна роль у телекомунікаційній галузі належить таким сегментам, як машинне навчання, глибоке навчання та обробка природних мов.

Машинне навчання (ML) - це підмножина штучного інтелекту, яка фокусується на комп’ютерній програмі, що має здатність аналізувати дані за допомогою конкретних алгоритмів. Така програма здатна модифікувати себе без участі людини, виробляючи бажаний результат на основі аналізованих даних. По суті, використовуючи методи ML, машина навчається аналізувати величезні обсяги даних, а потім вчиться виконувати конкретні завдання.

Глибоке навчання (DL) - це підмножина машинного навчання, алгоритми та методи якої подібні до машинного навчання, але можливості не є аналогічними. Основна різниця між ML та DL полягає в інтерпретації даних, якими вони харчуються. У DL комп'ютерна система навчена виконувати класифікаційні завдання безпосередньо зі звуків, текстів або зображень за допомогою великої кількості маркованих даних, а також архітектур нейронних мереж.

Обробка природної мови (NLP) - це підполе ШІ, яке орієнтоване на надання комп'ютерам можливості розуміти, інтерпретувати та маніпулювати людською мовою. По суті, NLP дозволяє машинам читати тексти, чути звуки, інтерпретувати їх та вимірювати почуття.

Коротко оглянемо декілька яскравих випадків використання ШІ саме для телекомунікацій.

Verizon Communications. Це одна з найбільших постачальників послуг криптографії у світі, яка інвестує значні кошти в технології AI / ML для покращення продуктивності мережі та обслуговування споживачів. Нещодавнє партнерство з оператором мобільної мережі Cellwize призвело до створення нової інтелектуальної платформи, що сприяє розгортанню сайтів Verizon 5G та спрощує розробку мережевих додатків.

Vodafone. Британський телекомунікаційний гігант Vodafone Group запустив новий додаток-помічник – це високоінтелектуальний текстовий бот, здатний підтримувати користувачів у вирішенні проблем, керуванні передплатою та придбанні нового обладнання та послуг.

Deutsche Telekom. Компанія робить значні інвестиції в ШІ на різних рівнях. Цей чат-сервер активно вбудовує елементи ШІ у свою інфраструктуру та портфель послуг, починаючи від чат-бота під назвою Tinka, який може надати понад 1500 відповідей на запитання клієнтів, до інтелектуальних інструментів бізнес-планування.

Література:

1. https://softengi.com/blog/ai-is-the-telecom-industry-trend-automatic-adaptive-autonomous/(дата звернення: 10.02.2020)

2. https://www.intellias.com/ai-in-telecommunications/ (дата звернення: 11.02.2020)

ЕЛЕКТРОННИЙ ПРИСТРІЙ ДЛЯ ЗАПОБІГАННЯ ВИКРАДЕННЯ АВТОМОБІЛЯ

Лаврінець Костянтин Григорович, Дмитренко Володимир Віталійович,
Кісельова Катерина Олександрівна, Марчук Ольга Миколаївна
Державний університет телекомунікацій
Науково-навчальний інститут Телекомунікацій
м. Київ

Дана стаття присвячена питанням, пов'язаним з удосконаленням систем охорони рухомого майна (автомобілів) громадян на основі новітніх інтелектуальних технологій телекомунікаційних систем.

Згідно рекомендаціям МСЕ все більше поширення набувають цифрові технології майбутнього на базі 4G/5G [1]. Вони властиві стрімкому розвитку телекомунікацій в різних галузях, в тому числі і в розробці сучасних автомобільних охоронних систем.

Для охорони автомобілів в наш час використовується складний комплекс, в якому присутні найсучасніші механічні, електронні та електронно-механічні пристрої.

Класифікувати ці пристрої можна наступним чином:

- механічні засоби (Mult-lock, Beer-lock, Construct та інші);
- електронні (автосигналізації, протиугінні пристрої, блокатори ланцюгів керування відповідними пристроями та агрегатами та інше);
- електронно-механічні (Hood-lock, Construct та інше).

В даній статті розглянуті тільки електронні пристрої. Їх перелік включає: автосигналізації (односторонні, двохсторонні, супутникові та GSM-сигналізації), іммобілайзери та блокиратори ланцюгів керування (живленням, запаленням, стартера, палива, педалі щеплення та інше).

Розроблений пристрій має ряд переваг над існуючими, наприклад BlagBug або SkyBrake. По-перше низьку ціну за рахунок використання доступних матеріалів (мікросхем, конденсаторів,транзисторів, опорів, перемикачів та інше), по-друге простота в використанні, по- третє проста процедура налагодження.

Розробка пристрою включала наступні процедури:

- розробка функціональної схеми;
- розробка принципової схеми;
- розробка монтажної плати;
- розробка зовнішньої упаковки;
- розробка інструкції з встановлення системи;
- розробка інструкції користувача.

Розроблений пристрій призначений для захисту автомобіля від викрадення. Перехід від ЧЕРГОВОГО РЕЖИМУ в режим блокування здійснюється програмно з часовим інтервалом 15с, 30с, 60с. Принцип роботи пристрою побудовано на вмиканні (вимиканні) ЧЕРГОВОГО РЕЖИМУ (режиму охорони), за рахунок чого забезпечується блокування (розблокування) ланцюга управління двигуном автомобіля.

Особливістю функціонування пристрою є те, що його активація здійснюється відкриттям двері водія. Часові інтервали спрацювання реле блокування програмуються при встановленні пристрою (заводське встановлення - 15 с). Індикація режимів

роботи пристрою здійснюється за допомогою багатофункціонального світло діода, звукових та світлових сигналів.

Якщо пристрій знаходиться в активному режимі, а підтвердження (натиснення потайної кнопки) відсутнє, спрацьовує реле блокування (двигун автомобіля блокується) та вмикаються світлові (як правило габаритні вогні) та звукові (сирена) індикатори.

Технічні характеристики пристрою:

- напруга живлення блоку управління (10-15В);
- струм живлення у ЧЕРГОВОМУ РЕЖИМІ (30 мА);
- максимальний струм навантаження, який комутує по виходу блокування запалення (40 А);
- кількість програмованих часових інтервалів (3);

Особливості користування пристроєм:

- увімкнення ЧЕРГОВОГО РЕЖИМУ пристрою здійснюється по відкриттю двері водія,а також за допомогою потайної кнопки або брелока автосигналізації, якщо остання встановлена на автомобілі
- відмінною властивістю пристрою є те, що навіть при зчитуванні коду авто сигналізації, що дозволяє зняти її з режиму охорони, пристрій залишається в ЧЕРГОВОМУ РЕЖИМІ та може бути розблокованим тільки за допомогою потайної кнопки
- індикація присутності ЧЕРГОВОГО РЕЖИМУ підтверджується відсутністю світловода; у ввімкненому стані він інформує водія, що ЧЕРГОВИЙ РЕЖИМ вимкнений.

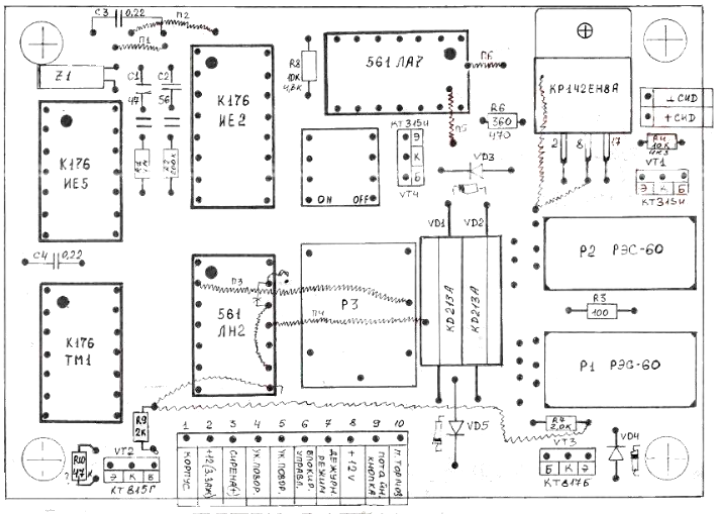


Рис.1 Функціональна схема пристрою

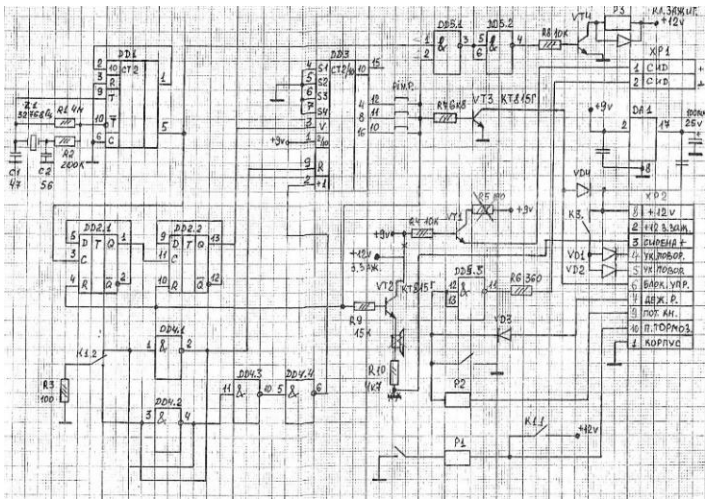


Рис.2 Принципова схема

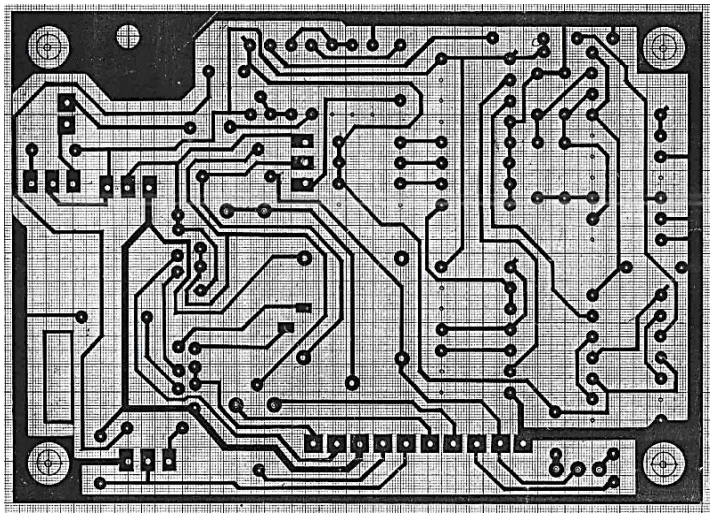


Рис.3 Монтажна плата

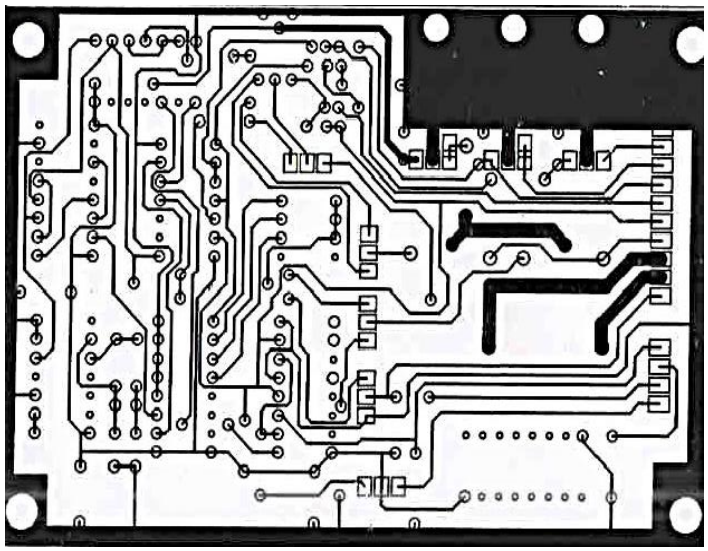


Рис.4 Монтажна плата (зворотній бік)

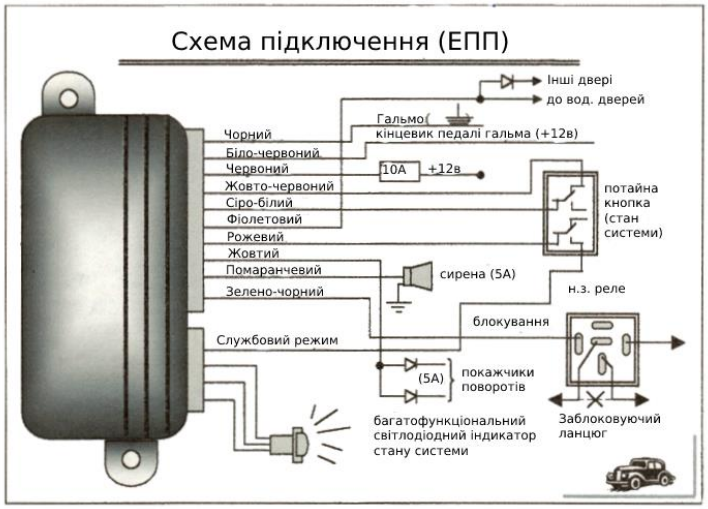


Рис.5 Схема підключення

Література:

1. Маркировка электронных компонентов. Определитель. Додека XXI, 2016 г.- стр.

2. Зарубежные микросхемы памяти и их аналоги. Справочник-каталог. Том 1. РадиоСофт, 2002 г.,-576 стр.

3. Садченков Дмитрий Андреевич. Маркировка радиодеталей. Том 1. СОЛОН-Пресс, 2010 г.-

стр.

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Локойда Андрій Олегович, Май Максим, Левін Микола Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Телекомунікаційні системи та мережі представляють складний комплекс різноманітних технічних засобів, що забезпечують передачу різних повідомлень на будь-які відстані із заданими параметрами якості. Основу телекомунікаційних систем складають багатоканальні системи передачі по електричних, волоконно-оптичних кабелях і радіолініях, призначені для формування типових каналів і трактів. На основі систем передачі будується телекомунікаційна мережа країни, що реалізується у вигляді комплексів технологічно сполучених мереж електрозв'язку загального користування, відомчих і приватних мереж електрозв'язку на території України.

Телекомунікаційні системи являють собою технічні засоби, призначені для передачі великих обсягів інформації через оптоволоконні лінії зв'язку. Як правило, телекомунікаційні системи призначені для обслуговування великої кількості користувачів: від декількох десятків тисяч до мільйонів. Використання такої системи передбачає регулярну передачу інформації в цифровому вигляді між усіма учасниками телекомунікаційної мережі. Головна особливість сучасного обладнання для мереж-забезпечення безперебійного з'єднання,

щоб інформація передавалася постійно. При цьому допускається Періодичне погіршення якості зв'язку в момент встановлення з'єднання, а також періодичні технічні неполадки, викликані зовнішніми факторами. [1, с. 3–4]

Сучасні телекомунікаційні системи об'єднуються за кількома основними ознаками. Залежно від призначення, розрізняються системи телевізійного мовлення, персонального зв'язку, а також комп'ютерні мережі. Залежно від технічного забезпечення, яке використовується для передачі інформації, виділяються традиційні кабельні комунікаційні системи, більш досконалі – оптоволоконні, а також ефірні і супутникові. [1, с. 5–6]

Комп'ютерні системи являють собою сукупність декількох ПК, об'єднаних в єдине інформаційне поле за допомогою кабелів і спеціалізованих програм. Сукупність встановленого обладнання та програмного забезпечення являє собою автономну саморегулюючу систему, яка обслуговує підприємство в комплексі.

Залежно від своїх функцій, обладнання комп'ютерної системи розділяється на:

- сервісне;
- активне;
- персональні пристрої.

Для забезпечення роботи всієї системи необхідно відповідне програмне забезпечення, належним чином налаштоване, виходячи з потреб користувачів. [4, с. 20–22]

Радіотехнічні та телевізійні системи. В основі радіотехнічних систем передачі повідомлень лежать електромагнітні коливання, які транслюються по спеціальному радіоканалу. Одиницею функціонування системи є сигнал, який перетвориться в передавальному пристрої і потім трансформується в інформаційне повідомлення в приймаючому пристрої. Основа безперебійного функціонування радіотехнічних систем є лінія зв'язку - фізичне середовище і апаратні засоби, які забезпечують своєчасну і повну передачу інформації. [2, с. 20–21]

Глобальні телекомунікаційні системи. До глобальних телекомунікаційних систем відносяться ті апаратні та програмні засоби, які з'єднують користувачів незалежно від їх фізичного стану на планеті. Головна риса глобальних мереж-інтелектуалізація, що дозволяє легко використовувати потужності мережі з оптимальною ефективністю, при цьому мінімізуючи витрати на обслуговування обладнання. Серед глобальних мереж виділяється кілька основних видів.Цифрові

мережі з інтегральними модулями використовують безперервну комутацію каналів, при цьому масиви даних обробляються в цифровій формі. Мережі X25 є найбільш старими, надійними і перевіреними технологіями передачі інформації між необмеженим числом користувачів. Головна відмінність таких мереж-наявність пристрою для» складання «окремих блоків переданої інформації в» пакети " для найбільш швидкої передачі.Асинхронний режим передачі даних-сучасна технологія, яка використовується для широкосмугових мереж, які засновані на оптоволоконних кабелях. [2, с. 22–24]

Оптичні телекомунікаційні системи. Основою оптичних телекомунікаційних систем є оптоволоконний кабель, який з'єднує окремі апарати в єдину глобальну мережу. Сигнали передаються за допомогою інфрачервоного діапазону випромінювань, при цьому пропускна здатність оптоволоконного кабелю перевищує показники інших видів обладнання.Технічні характеристики матеріалу забезпечують слабкий рівень затухання сигналу на великих відстанях, що дозволяє використовувати кабель для комунікації між материками. [2, с. 25–26]

Багатоканальні телекомунікаційні системи. Відмінною рисою таких комунікаційних систем є використання кількох каналів передачі інформаційних сигналів. Сучасні телекомунікаційні системи використовують кабельні, хвильові, радіорелейні, а також космічні лінії зв'язку. Зашифрований сигнал передається зі швидкістю в кілька гігабіт на секунду на величезні відстані.Головне достоїнство багатоканальних систем - забезпечення стабільної роботи. При виході з ладу одного каналу зв'язку, автоматично підключається наступний. Користувачі захищені від раптового обриву зв'язку і втрати важливої інформації. В основі таких систем лежать структуровані конструкції з кабелів. [2, с. 27–29]

Мультісервісні телекомунікаційні системи. Мультісервісні телекомунікаційні системи являють собою апаратну і програмну середу, призначену для передачі даних за технологією комутації пакетів - з'єднання окремих блоків інформації в повідомлення великого розміру. Особливість мультисервісних систем - необхідність забезпечення стабільної роботи всіх елементів транспортної середовища. Як правило, для передачі даних, а також мовної та відеоінформації використовуються різні технології, але при цьому інфраструктура єдина. Тому основний принцип побудови мультисервісних мереж - універсальність технологічного рішення, за допомогою якого обслуговується різнорідне

обладнання, призначене для виконання різних операцій. Мультісервісна система використовує єдиний канал для передачі даних різних типів. [2, с. 30–33]

Структура, обладнання та компоненти телекомунікаційних систем. В основі будь-якої телекомунікаційної системи лежать сервери, на яких зберігається і обробляється необхідна користувачам інформація. Серверні представляють собою невеликі приміщення з промислової вентиляцією, що забезпечують функціонування безлічі жорстких дисків великого обсягу. Комп'ютери користувачів є засобом зв'язку між базою даних і конкретними користувачами інформації, які здійснюють пошукові запити. Технічна основа телекомунікаційних мереж - це лінії зв'язку, тобто середовища передачі даних, в якості яких використовуються оптоволоконні, коаксіальні або бездротові канали зв'язку.

Мережеве обладнання, що забезпечує передачу і прийом даних:

- модеми;
- адаптери;
- маршрутизатори;
- концентратори;

Подібні пристрої доповнюють телекомунікаційну систему і необхідні для стабільної роботи. Програмне забезпечення дозволяє ефективно контролювати роботу встановленого обладнання, що забезпечує своєчасну передачу інформації в потрібних обсягах. [3, с. 51–55]

Майбутнє телекомунікаційних систем та мереж в 2021 році.

Наступні фактори матимуть ключовий вплив на індустрію в 2021 році. [4, с. 400]

1. Інтеграція

Зв'язок рухається в бік здешевлення. Вартість надання таких послуг продовжує знижуватися. З точки зору конкуренції це означає що ціна послуг знижується і знижується. Що стосується авторів контенту, послуг або продуктів - їх кількість зростає. Очікується, що одна або більше телекомунікаційних компаній будуть куплені авторами контенту на зразок Netflix. [4, с. 400–401]

2. Вибуховий розвиток парних пристроїв

Ще один фактор повного змінення індустрії - зростання інтернету речей. Речофікація додасть мільйони, а, можливо, й трильйони нових речей, підключених до інтернету. Як результат

- величезне збільшення обсягів передачі даних. Користувачі увійдуть в світ зетабайт. [4, с. 402–403]

3. Мобільність

Мобільний зв'язок розвивається по всьому світу і перевершує за обсягами кабельний зв'язок. Це пов'язують з тим, що зв'язок активно розвивається в більш бідних країнах та тих, що розвиваються. Жителі цих країн обґрунтовано вважають мобільні телефони більш доступними, корисними і простішими у використанні, не дивлячись на те, що кабельний зв'язок також доступний. [4, с. 404–405]

4. Насиченість

Світ стає все більш цифровим, що підвищує ефективність роботи. Користувачі будуть споживати все більше цифрових технологій, що збільшить обсяги трафіку до величи, до яких провайдери не готові. Як результат - ринок буде повністю насиченим. [4, с. 406–407]

5. Безпека

Провайдери зіткнуться з новими загрозами, які ростуть з кожним днем. Користувачі все більше дбають про безпеку комунікацій і захист персональних даних. Це призведе до підвищених вимог безпеки для провайдерів з боку користувачів. Провайдери в свою чергу будуть змушені впроваджувати нові технології захисту персональних даних щоб задовольнити вимоги безпеки для користувачів. [4, с. 408–409]

Література:

1. Телекомунікації. Керівництво для початківців. / Мур М., Прітск Т., Ріггс К., Сауфвік П. - СПб.: БХВ-Петербург, 2009 рік.

2. Ткаченко, А. П. Тенденції розвитку систем цифрового телевізійного мовлення / а. п. Ткаченко, М. і. Зорько, Д. А. Хатьков / Мінськ: БГУІР, 2014 рік

3. Комп'ютерні мережі. Принципи, технології, протоколи: підручник 4-е вид. / В.Г. Оліфер, Н.А. Оліфер-СПб. Пітер, 2010 рік.

4. Пєскова, С.А. Мережі та телекомунікації: підручник - М.: Academia, 2017 рік.

ДОДАТОК ASTERISK ЯК РІШЕННЯ ДЛЯ СТВОРЕННЯ МЕРЕЖІ IP- ТЕЛЕФОНІЇ

Макаренко Артем Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Додаток Asterisk – це вільне рішення комп'ютерної телефонії (в тому числ і VoIP) з відкритим вихідним кодом від компанії Digium, розроблене Марком Спенсером. Додаток працює на операційних системах Linux, FreeBSD, OpenBSD і Solaris і ін.

Asterisk в комплексі з необхідним обладнанням має всі можливості класичної АТС, підтримує безліч VoIP-

протоколів і надає багаті функції управління дзвінками, серед них: голосова пошта; конференц зв'язок; IVR (інтерактивне голосове меню); постановка дзвінків в чергу і розподіл їх по абонентам; Call Detail Record (докладний запис про виклик).

Для створення додаткової функціональності можна скористатися власною мовою Asterisk для написання плану нумерації, створивши модуль на мові Сі, або скориставшись Asterisk Gateway Interface - гнучким і універсальним інтерфейсом для інтеграції з зовнішніми системами обробки даних. Модулі, що виконуються через AGI, можуть бути написані на будь-якій мові програмування.

Додаток Asterisk може працювати як з аналоговими лініями FXS-модулі), так і цифровими (ISDN, BRI і PRI - потоки T1 / E1). За допомогою певних комп'ютерних плат (найбільш відомими виробниками яких є Digium, Sangoma, OpenVox, Rhino, AudioCodes) Asterisk можна підключити до високопропускних ліній T1 / E1, які дозволяють працювати паралельно з десятками телефонних з'єднань. Повний список обладнання для з'єднання з телефонною мережею загального користування визначається підтримкою обладнання в модулях ядра, наприклад DUNDi.

Додатком Asterisk підтримуються наступні протоколи:

- SIP;
- H.323;
- MGCP;
- XMPP;
- IAX2;
- SIMPLE;
- Skinny / SCCP;
- Unistim.

Додаток дає можливість транслювати текст і відеосигнали (наприклад, використовувати відеофон). Крім того, реалізована робота з іншими комп'ютерними протоколами: DUNDi; OSP; T.38.

Підтримка широкого спектру обладнання та комп'ютерних протоколів дозволяє організовувати величезну кількість сценаріїв взаємодії мереж, отримання і обробки інформації.

Налагодження та програмування додатку проводиться за допомогою декількох механізмів: використанням спеціальних мов програмування (AEL; Lua), а також AGI та AMI.

Розширення виконуваних функцій також можливо шляхом написання на мові Сі нового модуля, що можливо завдяки докладної Doxygen-документації.

Література:

1. Огляд вільно доступних і безкоштовних IP АТС [Електронний ресурс] // –

Режим доступу: https://habr.com/ru/post/122215/
2. *Asterisk [Електронний ресурс] // – Режим доступу: https://www.asterisk.org*

COVID-19'S IMPACT ON THE GLOBAL TELECOMMUNICARIONS INDYSTRY

Mantula Roman
State University of Telecommunications
Educational and Scientific Institute of Telecommunucation
Kyiv

The COVID-19 pandemic—perhaps more than any other event in human history— has demonstrated the critical importance that telecommunications infrastructure plays in keeping businesses, governments, and societies connected and running. Because of the economic and social disruption caused by the pandemic, people across the globe rely on technology for information, for social distancing, and working from home.

The telecommunications sector has seen tremendous technological advances over the past few decades, with mobility, broadband, and internet services growing in capability and reach across the globe. The International Telecommunication Union (ITU) estimates that there were over 4 billion internet users at the end of 2019, of which over 3 billion users are in developing countries. However, in spite of progress in access to internet and mobile services, many people and businesses remain disconnected. Globally, 3 billion citizens remain unconnected. And in Africa, only 294 million have internet access out of a population exceeding 1 billion. IFC supports projects that bridge these gaps.

C1: The telecommunications services industry consists of digital infrastructure (such as fiber, telecommunications towers, active networks, and data centers), operators (mobile and fixed broadband, data centers, and cloud computing), and applications (broadband connections, telephony, video, e-commerce, and others). The sector holds promising opportunities for private sector investors.

C2: Many telecom players — from broadband to mobile to data center operators — have benefitted from a surge in the traffic of data and voice.

C3: In the face of the uncertain future, our clients are trying to strike a balance between expanding to meet higher demand in the short-term and preserving cash to weather a protracted economic downturn

C4: An extended pandemic will have an increasing impact on the global economy, affecting the financial health of consumers and businesses and hence long-term demand. Mobile and broadband operators with strong exposure to retail consumers may suffer more in the short term, but the damage will eventually have an impact

throughout the value chain. The impact will hinge on how long the lockdown will last.

SECTOR BACKGROUND

The telecommunications services industry consists of digital infrastructure (such as fiber, telecommunications towers, active networks, and data centers), operators (mobile and fixed broadband, data centers, and cloud computing), and applications (broadband connections, telephony, video, e-commerce, and others). The sector holds promising opportunities for private sector investors.

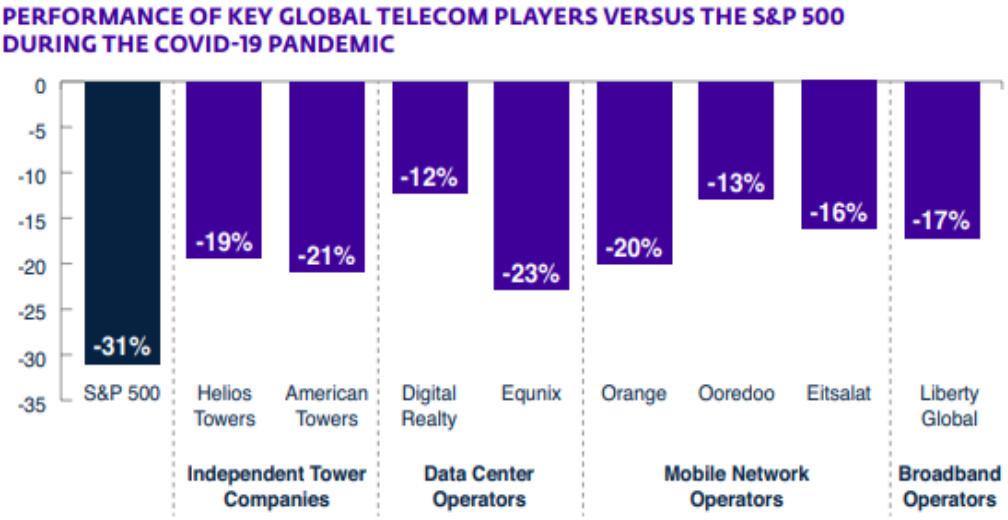
The sector has remained "mission-critical" to keep economies moving under the lockdown in at least three different ways:

1. Providing business-critical connectivity and resiliency;
2. Facilitating work-from-home arrangements;
3. Keeping individuals and societies connected and informed, with access to medical, financial, commercial, and other essential services during mandated social isolation.

COVID-19'S IMPACTS ON THE SECTOR

Many telecom players—from broadband to mobile to data center operators—have benefitted from a surge in the traffic of data and voice. As a result, the telecom sector is performing well compared to other infrastructure sub-sectors.

In sharp contrast to many other industries, the telecommunication sector has been generally exempted from major COVID-19-related restrictions, such as stay-at-home orders and quarantine requirements, as it is recognized as an essential service. Some telecom companies have been strengthened by the short-term spike in data traffic and increased use of broadband services, as more people are working from home and rely on video conferencing to hold meetings. Traffic growth has, in fact, demonstrated increased reliance on connectivity and digital services. As a result, the telecom sector has remained acyclical relative to the S&P 500 throughout the crisis, as shown below:



Source: S&P Capital IQ. Note: Based on the difference between the closing prices on February 21, 2020, when the stock market was first impacted by the pandemic, and March 20, 2020, when the stock market started to stabilize; all data retrieved from S&P Capital IQ.

The technology, media, and telecom (TMT) sector, however, is not isolated from short- or medium-term disruptions. General macroeconomic impacts, restrictions in distribution of airtime, and demand shortfalls from the bottom of the pyramid are beginning to have an effect. To find out what impact COVID-19 has had on the TMT sector—and the implications for future business—IFC interviewed 20 of its telecom partners and clients. Specifically, we looked at short- and medium-term impacts across four key elements of the value chain: network buildout, operation and maintenance, service commercialization, and financing. Our findings are as follows:

NETWORK & FACILITY CONSTRUCTION

Short-term construction is generally exempted from containment measures. Given the critical nature of telecommunications, many of our clients in developing countries are permitted to carry out construction. Some of our eastern European clients report a more favorable construction environment than usual due to a surge of available workers.

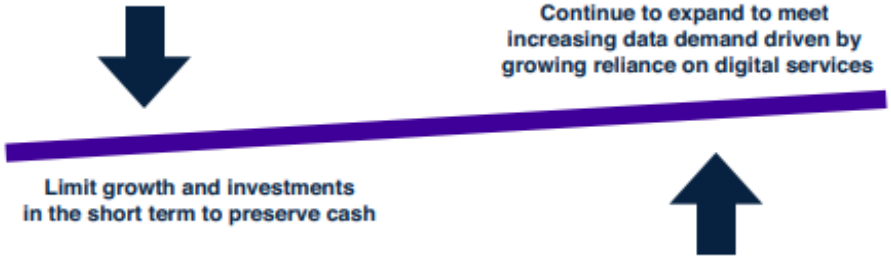
Short-term supply disruptions are expected to recede in the second half of 2020. The risk of further delays in shipments of network equipment is considered small.

Some clients may voluntarily suspend construction due to supply chain disruptions. A lack of materials and equipment—particularly those imported from China—has prompted some clients to suspend new construction. However, affected clients are well-stocked on critical inventory. They estimate that 70–80 percent of

Chinese suppliers have resumed to usual operations and are optimistic that construction can resume within 2–4 weeks.

Resolution of service-level agreements (SLAs) affected by production delays still unclear. The construction cuts and delays are impacting SLAs and delivery timelines. Clients may commit to upholding offtake obligations and request compensations for delays. Alternatively, they may agree with wholesale infrastructure companies to postpone the delivery timeline or even cancel partially constructed projects. In most cases, the impact will be a change in the delivery schedule without significant penalties.

Growth-stage clients are most impacted. IFC clients that rely on significant construction for revenue growth are most impacted. For clients not currently undergoing large-scale construction projects or having a diverse revenue base, such disruption is very limited.



OPERATIONS AND MAINTENANCE

Operations and maintenance remain largely uninterrupted. No extended period of interruption was reported by clients, who are generally confident about continuing normal service levels and operational performance. Governments across emerging markets typically allow suppliers to continue with maintenance work because of the need for connectivity during the quarantine. Most clients are well-stocked on critical inventory, which protects them from supply chain disruptions. However, if containment measures—namely, lockdowns—continue or escalate in some emerging markets beyond July 2020, our clients' ability to maintain network quality may be compromised.

Service levels are not experiencing significant disturbances. Most clients have effective business continuity plans, effective operational procedures, and supply agreements for key processes. As a result, operational performance is normal, with service levels exceeding 99.95 percent.

Contingency plans enable firms to manage spiked demand during the quarantine. The data load challenge has generally been manageable. As people move away from city centers amid the work-from-home arrangement, data density has become more scattered,

and thus networks have become less congested. If demand exceeds capacities, our telecom clients have the option to request over-the-top service providers (OTTs) to throttle usage, reduce speed, and lower qualities to ensure service levels.

SERVICE COMMERCIALIZATION

Telecom demand spikes are leading to short-term revenue upticks. Our operator clients— including mobile network operators (MNOs) and internet service providers (ISPs)—are experiencing an uptick in revenue from increased usage. This benefit is shared across the telecom value chain. None of our infrastructure clients reported termination of major customer contracts due to COVID-19 despite furloughs and temporary closing of businesses.

Continuous growth and business development are uncertain in the foreseeable future. The lockdown has affected the movement of salespeople and distributors, significantly increasing the difficulties for new business development. Some operators are reporting reductions in retail revenue as points of sale for prepaid services are shut down, although some sales were recouped through online channels. Additionally, due to the slowdown of the global economy, most of our clients' business customers are reluctant to commit to new contracts or purchase handsets.

The general creditworthiness of customers has declined. As a result of the lockdown, most high-value enterprise customers—including schools, universities, hotels, restaurants, and offices—have stopped operations and face liquidity challenges. Some customers—particularly small and medium businesses—have requested a temporary suspension of services, rebates, discounts, or payment holidays.

Revenues may decline due to reduced economic activity in the medium term. Because customers generally prioritize telecom services over other expenses, the potential decline in telecom services is expected to be lower than other discretionary spending.

FINANCING

Foreign exchange (FX) carries the most direct financial risk. COVID-19 and the recent decline in oil prices are putting pressure on emerging market currencies and economic growth. However, most clients have not seen solvency risks triggered by currency depreciation thus far. Neither did they encounter significant issues on the conversion of local currency to meet payment obligations offshore. MNOs will feel the FX impact immediately as their revenues are denominated in local currencies. Other clients, such as tower and data center companies, mostly have five to ten-year contracts denominated in hard currencies, but are exposed to FX risk

indirectly through the creditworthiness of their MNO clients. Clients also expect significant FX effects on the price of imported network equipment.

Efforts to raise capital may be delayed. Companies raising private capital are considering options to avoid drops in valuations related to uncertainties. Merger and acquisitions (M&A) activities have also stalled as buyers have become increasingly prudent in using cash.

Uncertain The outlook in the bond market is uncertain. Some of our clients have reported difficulties accessing bond markets, especially firms that are non-investment grade.

RESPONSE TO THE CRISIS

In the face of the uncertain future, our clients are trying to strike a balance between expanding to meet higher demand in the short-term and preserving cash to weather a protracted economic downturn.

Amid uncertainties, clients have mixed sentiments about new deployment for network and facility construction. Most clients have already purchased and shipped additional equipment to construction sites. However, some clients are expected to be prudent, slowing down deployments in response to uncertainties. Others see the demand spikes as new opportunities for growth. This latter group has reported more confirmed orders over the past few weeks and plans to capitalize on the opportunity to exceed their business plan for 2020, making the most of depleted labor prices.

Lower-income customer groups, who are experiencing the most damage, are expected to reduce or stop purchasing airtime and data bundles. However, the increased consumption by higher-income customer groups, mainly driven by higher data consumption, may partially offset the decline in the bottom segment.

MNOs are reluctant to commit to new wholesale contracts with infrastructure operators.

Infrastructure operators such as tower companies and energy service companies (ESCOs) may see a drop in new MNO contracts. Their MNO clients will likely become less willing to take risks on network expansion or continuing switchover of 3G equipment to 4G, and pause any consideration of 5G deployments.

MNOs facing issues with collections from business and consumer customers are likely to request a delay in payments to their infrastructure services. Clients anticipate payment delays from an average of 45 days to up to 90 or 120 days. This creates the need for additional working capital.

Industry consolidation and capital raise may intensify in the long term. Some clients have pointed out the potential for industry

consolidation in the longer term and expect M&As to ramp up, starting from the second half of 2020.

GOING FORWARD AND IFC SUPPORT

An extended pandemic will have an increasing impact on the global economy, affecting the financial health of consumers and businesses and hence long-term demand. Mobile and broadband operators with strong exposure to retail consumers may suffer more in the short term, but the damage will eventually have an impact throughout the value chain. The impact will hinge on how long the lockdown will last.

Most clients expressed confidence in managing the pandemic. Notwithstanding, some have expressed concern for the medium term if the pandemic persists, and have asked for support from IFC.

In response, IFC is in the process of accelerating investments in excess of $400 million to support our existing clients in the telecommunications sector. The financing will be utilized to address working capital requirements, refinance debt maturing in the short term and support network expansion through long grace periods and tenors. IFC's support of the telecommunications sector is part of IFC's $8 billion in fast-track financing. Of this, the Real Sector Crisis Response Facility is providing $2 billion to support clients in the infrastructure, manufacturing, agriculture, and services industries, including TMT.

Literature:

1. https://www.ifc.org/wps/wcm/connect/1d490aec-4d57-4cbf-82b3-d6842eecd9b2/IFC-Covid19-Telecommunications_final_web_2.pdf?MOD=AJPERES&CVID=n9nxogP

ЗВ'ЯЗОК МІЖ ОСНОВНОЮ МОДЕЛЛЮ NGN І РЕКОМЕНДАЦІЯМИ ITU-T

Марчук Ольга Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

У даній статті розглянутий зв'язок між основною моделлю NGN і рекомендаціями ITU-T. В основу концепції побудови NGN покладено ідею про створення універсальної мережі, яка б дозволяла переносити будь-які види інформації, такі як мовлення, дані, відео, аудіо, графіку тощо, а також забезпечувати можливість надання самого широкого спектра інфокомунікаційних послуг. ITU-T уже почав стандартизацію мереж нового покоління в рамках проекту глобальної інформаційної інфраструктури, що привело до розробки низки Рекомендацій з GII серії Y. Однак питання практичної реалізації не входять до сфери GII. Тому Рекомендації з GII мають бути доукомплектовані додатковими технічними вимогами щодо впровадження в практику конкретних реалізацій NGN.

Функціональні принципи архітектури рек. G.805 і G.809 можуть бути застосовані до вертикального зв'язку між багаторівневими мережами в рамках однієї мережі NGN, а підходи, викладені в рек. Y.110, - до оцінки ролі, гравців і організацій в корпоративної моделі (Enterprise Model), до сервісів і додатків в структурній моделі (Structural Model), до функцій і інтерфейсів в функціональної моделі (Functional Model) і до компонентів в моделі реалізації (Implementational Model).

Узагальнена мобільність - можливість для користувача (або іншого мобільного об'єкта) спілкуватися і мати доступ до сервісів незалежно від зміни їх положення або технічного оточення. Ступінь можливості бути обслуговуваним може залежати від ряду факторів, включаючи можливості конкретної мережі доступу, угод про рівень обслуговування (якщо такі є) між базовою чи домашньою мережею користувача і візитною мережею і т.д. Мобільність включає можливість зв'язку з безперервним обслуговуванням або без обслуговування.[1]

Загальна функціональна модель

Рек. Y.110 формалізує структурну модель, де сервіси та їх компоненти описуються окремо, забезпечуючи:

- корпоративну модель, яка встановлює гравців і їх структурні та інфраструктурні ролі, тобто бізнес-активності в рамках послідовності нарахування вартості (value chains);
- модель реалізації, яка сконцентрована на тому, як функції моделі розподіляються і реалізуються обладнанням; вона визначає протоколи, які обслуговують інтерфейси між елементами обладнання. В даному контексті це розглядається як фізична реалізація мережі NGN.[1]

Як і GII, мережа NGN повинна розділяти аналіз сервісів і функцій. Рек. Y.110 може бути використана як посібник для декомпозиції на інфраструктурні та прикладні сервіси, сервіси Middleware і Baseware. Рек. G.805, G.809, G.807 / Y.1302, M.3010, M.3400, M.3050.x, X.700 і X.701 були розроблені для освітлення функціональних аспектів (транспортної) мережевої операції. При вивченні NGN їх слід брати до уваги, а їх зв'язки між функціями, сервісами і ресурсами повинні бути встановлені для обох шарів NGN.[2]

Ці сервіси і функції пов'язані між собою, так як функції зазвичай вбудовані в сервіси. Більш того, існує певна схожість між підтипами цих сервісів і функцій. Однак немає однозначної відповідності між функціями і сервісами, і це одна з причин, чому вони повинні розглядатися окремо. Одна і та ж функція (наприклад, аутентифікація користувача) може бути

використана для доставки двох різних сервісів (Рек. Y.110, де представлені інфраструктурні та прикладні сервіси; сервіси middleware і baseware, включаючи зв'язкові сервіси і ресурси - компоненти сервісів обробки і збереження).

Зручно об'єднати ці функції в дві групи або площини: одна охоплює всі функції управління, а інша - всі функції менеджменту. Групування функцій одного і того ж типу (тобто управління і менеджменту) дає можливість визначити функціональні взаємозв'язки всередині заданої групи, а також інформаційні потоки між функціями в цій групі. Узагальнено це показано на рис.1, який дає уявлення про загальну функціональну модель.

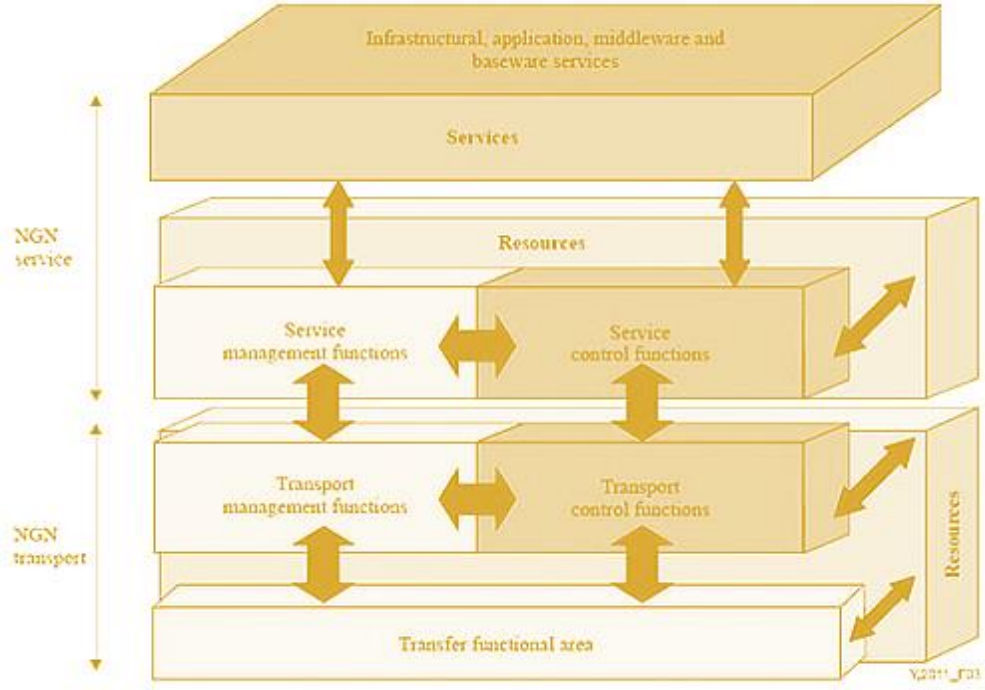


Рис.1 Загальна модель функціонування мережі NGN

Отже, можна зробити наступний висновок, що даний малюнок показує (в тривимірному вигляді) зв'язок між сервісними ресурсами і функціями сервісного шару NGN, з одного боку, і транспортними ресурсами і функціями транспортного шару NGN - з іншого. Зауважимо, що малюнок показує розділені площини управління і менеджменту, але не показує можливі загальні функції для сервісного і транспортного шарів.

Література:

1. ITU-T Recommendation Y.110 – Global Information Infrastructure principles and framework architecture, 1998.

2. ITU-T Recommendation G.805, G.809, G.807/Y.1302, M.3010, M.3400, M.3050.x, X.700, X.701.

3. Телекомунікаційні системи та мережі. Том 1. Структура й основні функції. / Зміст / Розділ 2. Мережі зв'язку наступного покоління: архітектура, основні

характеристики й послуги / Тема 2.1. Визначення й характеристика основних можливостей NGN 1 – Режим доступу до ресурсу: https://www.znanius.com/3573.html.

МЕТОДИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ WIMAX ДЛЯ ПОБУДОВИ МЕРЕЖ

Мелконов Роман Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Системи дротового цифрового зв'язку, які існують сьогодні, вже не можуть повною мірою задовольняти зростаючі потреби високошвидкісного широкосмугового доступу. Найважливішими їх недоліками є тривалі терміни прокладання, складності розширення, високі витрати, проблема «останньої милі». Застосування високошвидкісних цифрових з'єднувальних ліній DSL (Digital Subscriber Line) не знімає цієї проблеми.

WiMax – одна з технологій, покликаних вирішити проблему широкосмугового доступу до транспортних мереж, а до того ж, позбавити користувачів необхідності провідного підключення. WiMax повинен забезпечити високошвидкісний, захищений бездротовий доступ з підтримкою контролю над якістю на периферії мережі. Ця технологія не є втіленням принципово нової концепції, її варто розглядати як еволюційний розвиток існуючих раніше технологій широкосмугового бездротового доступу (ШБД). Основна перевага WiMax – наявність загальноприйнятого стандарту, який дозволяє виробникам працювати над однією технологією, забезпечуючи взаємну сумісність обладнання.

Мета технології WiMax полягає в тому, щоб надати універсальний бездротовий доступ для широкого спектра пристроїв (робочих станцій, побутової техніки «розумного будинку», портативних пристроїв і мобільних телефонів) та їх логічного об'єднання – локальних мереж. Для постачальників послуг WiMax, а також для проектувальників мереж важливо знати, яку територію покриває зона дії станцій WiMax.

Література:

1. WiMax технологія бездротового зв'язку: теоретичні основи, стандарти, застосування / [В. І. Сюваткін, В. І. Єсиненко, І. П. Ковальов, В. Г. Сухоребра]. – СПб. :БХВ-Петербург, 2005. – 368 с.

2. Форум WiMax. Методологія WiMax. Система оцінки. – 2007. – 2012 с

ПЕРСПЕКТИВИ РОЗВИТКУ ESIM В УКРАЇНІ

Осипець Олексій Анатолійович
Державний університет телекомунікацій

Українські оператори зв'язку активно розвивають свої мережі та надають абонентам найсучасніші послуги. Одним з них є eSIM, який, як очікується, підтримають тисячі абонентів по всій країні.

Ця технологія вже працює в 90 країнах світу. Кількість операторів, готових до його впровадження, щомісяця зростає. Незабаром eSIM стане звичним явищем, яке значно замінить зовнішні SIM-карти.

Технологія "прибула" в Україну наприкінці 2019 року. Нещодавно основні мобільні оператори України приєднались до операторів, які надають своїм клієнтам можливість відмовитися від фізичних SIM-карт. Вони запустили послугу міграції eSIM для найпопулярнішої категорії своїх передплачених клієнтів.

Головною особливістю eSIM є те, що завдяки цій технології вам більше не доведеться шукати найближчий магазин стільникових телефонів, щоб придбати пластикову SIM-карту.

SIM-картки - це застарілий формат, позбутися якого непросто через їх широке використання. Однак виробники смартфонів (і в даний час найбільші мобільні оператори у всьому світі) впроваджують підтримку eSIM.

Перехід на нову технологію дозволить:

- змінити постачальника послуг за лічені хвилини;
- зберігати профілі абонентів кількох операторів одночасно і змінювати їх, якщо потрібно, в налаштуваннях телефону;
- додатково захистити свій смартфон та номер мобільного телефону. Вбудовану SIM-карту неможливо просто видалити або вимкнути без облікових даних власника;
- скористатися послугами декількох операторів, якщо у вашому телефоні є лише один слот для SIM-картки.

eSIM - це технологія, яка відображає новий етап у розвитку мобільних мереж. Це зручно як для мобільних операторів, оскільки полегшує розповсюдження та активацію SIM-карт, так і для користувачів, оскільки розширює можливості управління тарифами.

Деякі експерти зазначають, що незабаром ця технологія стане головним каталізатором зниження вартості роумінгу. Абоненти зможуть вибрати найбільш зручні формати зв'язку та швидко переключатися між операторами, перебуваючи за кордоном.

Незважаючи на те, що технологія довела свою можливість і активно впроваджувалася операторами мобільного зв'язку, виробники смартфонів все ще відстають у цьому плані. У 2020 році лише флагманські продукти провідних брендів (Apple, Samsung, Google, Huawei, Motorola) отримають необхідні модулі.

У телефонах масового ринку такої технологічної новинки немає. Але інші персональні пристрої також мають вбудовані SIM-карти, а саме:

- Смарт-годинники (Samsung Gear S2 Classic 3G, Apple Watch, Xiaomi Mi Watch, починаючи з Series3);
- Планшети Apple (iPad Pro 11 і 12, Air 3, mini 5);
- Концептуальний ноутбук (HP Spectre Folio, Lenovo Yoga 630).

У дуже компактному корпусі розумних годинників навіть у маленької нано-SIM-картки немає місця для слота. Тому вбудований чіп є хорошим рішенням.

На мою думку, eSim має широкі перспективи на ринку пристроїв IoT. З бурхливим розвитком Інтернету речей деякі користувачі стикалися з труднощами при обслуговуванні великої кількості SIM-карт. Перехід на eSim розширює можливість дистанційного керування датчиками, камерами, SIM-картами в датчиках та інших пристроях.

Література:

1. Лазоренко Л.В. Аналіз ринку мобільного зв'язку України та напрямки його розвитку / Л.В. Лазоренко // Глобальні та національні проблеми економіки.– 2017.– №15. – С. 246–249.

2. 1. Цхведіани В. Телекомунікації України – перспективи розвитку та основні проблеми / В. Цхведіани // Фондовий ринок. – 2000. – № 16. – 208 с.

3. Васильєва Н. Основні тенденції розвитку ринку інформаційних технологій і комунікацій / Н. Васильєва // Економіст. – 2003. – № 10. – 94 с .

ЕКОНОМІКА РОЗВИТКУ IP-ТЕЛЕФОНІЇ

Осипець Олексій Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Нещодавно обговорена концепція майбутньої мережі, скорочено NGN (мережа наступного покоління), поступово стала концепцією IMS (мультимедійна підсистема IP). Концепція IMS дозволить мобільним операторам ефективно впроваджувати інноваційні мультимедійні послуги, використовуючи уніфіковану архітектуру та сервісні платформи.

Багато користувачів більше не бояться терміну VoIP, який є технологією, за допомогою якої ви можете здійснювати голосові дзвінки, передаючи Інтернет-трафік. Розвиток цього виду послуг розпочався з багатьма провайдерами "карткової телефонії" (коли підключення VoIP вимагало придбання пластикової картки та здійснення дзвінка в телефонний пул оператора), і зараз воно стало значною частиною ринку телекомунікацій. І деякими з цих послуг користуються не великі компанії, а приватні клієнти.

В даний час на ринку доступно кілька сотень програмних рішень для VoIP - таке програмне забезпечення портативно називається Softphone, і головне його завдання - імітувати всі функції звичайного, «залізного» IP-телефону на комп'ютері користувача. Використання таких програм виправдано як користувачами настільних комп'ютерів, так і тими, хто проводить значну кількість часу в дорозі - економія на використанні сучасних технологій з метою зменшення комунікаційних витрат видається цілком обгрунтованою.

Одна з найбільш перспективних сфер використання VoIP - мобільні термінали. Розглядаючи нововведення провідних виробників, можна побачити цікаву закономірність - усі виробники, будь то Nokia, SonyEricsson, Samsung чи Motorola, чудово розуміють, що, отримуючи доступ до мереж 3G/4G, користувачі будуть надсилати голосовий трафік через Інтернет. Замість традиційного способу в стільникових мережах, як це відбувається сьогодні. Крім того, якщо це можливо, вони віддадуть перевагу технології HSDPA зі швидкістю передачі даних у реальній мережі до 1,8-3,6 Мбіт / с та Wi-Fi.

У той же час, для операторів фіксованої телефонії IMS дозволяє оптимально інтегрувати телефонну послугу з IP-інфраструктурою, не тільки надаючи VoIP-послуги своїм абонентам, але також пропонуючи широкий спектр мультимедійних послуг, які можуть бути реалізовані за допомогою стандартних компонентів IMS. Можливість передачі мультимедійного трафіку з необхідною якістю забезпечується протоколом SIP, особливістю якого є встановлення сеансу обміну даними з резервуванням пропускної здатності на весь час обміну.

Архітектура IMS - це набір логічних функцій, які можна розділити на три рівні: рівень обладнання абонента та шлюзу, рівень управління сеансами та рівень додатків.

На рівні пристрою та абонентського шлюзу сигналізація SIP ініціюється та припиняється, що потрібно для встановлення сеансів та надання базових послуг, таких як перетворення мови

з аналогового або цифрового в пакети за допомогою транспортного протоколу реального часу (RTP). На цьому рівні існують медіа-шлюзи, які перетворюють основні VoIP-потоки в TDM-телефонію при взаємодії з традиційними мережами. Один мультимедійний сервер може працювати для потреб декількох служб, що дозволяє значно оптимізувати мережеву інфраструктуру.

На рівні управління викликами та сеансами існує функція управління сеансом викликів CSCF, яка реєструє абонентські пристрої та надсилає сигнальні повідомлення SIP на відповідні сервери додатків. Функція CSCF взаємодіє з рівнем транспорту та доступу, щоб забезпечити якість обслуговування всіх послуг.

SIP (Session Initiation Protocol) обраний основним протоколом для взаємодії елементів мережі в рамках концепції IMS завдяки властивій йому простоті, гнучкості та хорошій розширюваності. IMS включає багато серверів додатків, які надають як звичайні телефонні послуги, так і нові послуги (обмін миттєвими повідомленнями, миттєвий багатоточковий зв’язок, потокове передавання відео, мультимедійні повідомлення тощо).

Архітектура IMS була розроблена для використання в стільникових мережах третього покоління. Підтримка SIP забезпечує уніфікований підхід до розгортання та доступу до програм, а також інтеграції програм, що надаються третіми сторонами (наприклад, постачальниками вмісту).

Інтенсивний розвиток великого числа додатків, що використовують SIP, викликав необхідність збудування масштабованої мультисервісної інфраструктури, яка розділяла би транспортний рівень, рівень послуг і рівень керування.

Використання SIP дозволяє перейти до горизонтальної схеми організації послуг та підтримки різних технологій доступу.

Факти довели, що майбутнє IP-телефонії пов'язане з протоколом SIP. У 2001 році, через два роки після появи SIP, він був обраний основою для роботи мобільної мережі третього покоління, що фактично призвело до появи архітектури IMS.

Виробники телекомунікаційного обладнання розробляють і виготовляють шлюзи SIP, телефони SIP, сервери додатків та інші пристрої з підтримкою SIP. Сьогодні до списку компаній, що беруть участь у просуванні рішень IMS, входять Alcatel, Convade Technologies, Ericsson, Huawei Technologies, Lucent Technologies, Motorola, Nortel, Siemens тощо.

Література:

1. В.А. Фрейнкман. Эволюция технологий предоставления услуг IN в современных и перспективных сетях святи,: Технологии и средства связи. Специальный выпуск «АТС. Коммутационное оборудование, 2006.

2. Д.Девидсон и др. Основы передачи голосовых данных по сетям IP, 2-е изд.: Пер. с англ. – М.: 000 "И.Д. Вильяме", 2007. – 400 с.: ил.

ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Панченко Владислав Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Сучасний і надійний обмін інформацією визначає потребу в побудові ефективної мережевої інфраструктури, яка повинна задовольняти зростаючим вимогам організації. В умовах стрімкого зростання кількості користувачів інформаційних систем і обсягу обчислень, головними якостями корпоративних мереж передачі даних стають продуктивність, масштабованість, безпека і керованість мережі

Історія розвитку телекомунікаційних систем та мереж

Рівень інформатизації будь-якої країни, ступінь її залучення до глобального інформаційного суспільства (ГІС) визначається передусім розвитком інфокомунікацій. Основу інфокомунікацій формують інформаційні мережі, які, у свою чергу, базуються на телекомунікаційних мережах. Це найскладніші й найбільш інтелектуально насичені системи.

На шляху еволюційного розвитку телекомунікаційних систем та мереж прийнято виокремлювати три етапи: аналоговий, цифровий та етап телекомунікаційно-комп'ютерної інтеграції.

Із появою нових телекомунікаційних технологій, орієнтованих на пакетний спосіб передавання інформації, використання різних середовищ передавання (оптичне волокно,радіочастотний ресурс) та забезпечення мобільності зв'язку, виникла можливість суттєво підвищити продуктивність, ефективність та якість обслуговування телекомунікаційних мереж, а також розширити діапазон послуг, які ними надаються.

Телекомунікаційна мережа

Загальне поняття «телекомунікації» базується на уявленні про засоби, які дозволяють організувати зв'язок між двома і більше віддаленими пунктами.Секція телекомунікацій Міжнародного союзу електрозв'язку (Telecommunications Standardization Sector of International Telecommunications Union, ITU-T) у Рекомендаціях серії I (I.110, I.112) визначає термін «телекомунікації» (Telecommunications) як сукупність засобів,

які забезпечують перенесення інформації, поданій у необхідній формі, на значну відстань за допомогою поширення сигналів в одному з середовищ (міді, оптичному волокні, ефірі) або сукупності середовищ.

Засобами, визначеними загальним поняттям «засоби телекомунікацій», є лінії зв'язку, пристрої з'єднання середовищ, системи передачі, комунікаційні пристрої мережі, обладнаннясигналізації, синхронізації та ін. Таким чином, телекомунікаційна мережа (Telecommunication Network, TN) – це системоутворююча сукупність засобів телекомунікацій, що надає територіально віддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо).

Загальні принципи організації телекомунікаційних мереж. Мережі операторів зв'язку

Сьогодні мережі операторів зв'язку є рушійною силою і місцем прикладання практично всіх нових транспортних технологій телекомунікаційних мереж. Корпоративні мережі, як правило, вже не будуються на основі власної інфраструктури глобальних зв'язків –тепердля об'єднання локальних мереж своїх територіально розосереджених підрозділів підприємства звертаються до транспортних послуг телекомунікаційних мереж операторів зв'язку.

Оператором зв'язку (Telecommunication Carrier) називається компанія, яка є власником телекомунікаційної інфраструктури та бере на себе всі витрати щодо забезпечення її працездатності з заданим рівнем якості обслуговування. Її ще називають мережевим оператором, або просто оператором.

Оператори зв'язку відрізняються один від одного:

• набором наданих послуг;

• територією, в межах якої надаються послуги;

• типом клієнтів, на яких орієнтовані їхні послуги;

• наявною у володінні оператора інфраструктурою – лініями зв'язку, комутаційним обладнанням, інформаційними серверами і т. п.

Література:

1. *https://core.ac.uk/display/161261756*
2. *https://amrita-cs.com/telecommunication_systems/*

ОПТОВОЛОКНО ЯК СЕРЕДОВИЩЕ ПЕРЕДАЧІ ДАНИХ

Пелехай Сергій Віталійович

Державний університет телекомунікацій

Навчально-науковий інститут Телекомунікацій

Оптичне волокно складається з прозорого сердечника - середовища передачі світла, і оболонки (демпфера), яка перешкоджає загасання імпульсу і забезпечує його доставку до кінцевої точки.

Передаючі середовища, які інакше називають ядрами оптичних волокон, роблять із кварцового, халькогенидного та інших видів скла, а також з акрилових смол. Ці матеріали характеризуються міцністю, гнучкістю, високою світлопроникністю і низькою чутливістю до перепадів температур і випромінювання. Оболонки також складаються зі скла або пластику [3].

У волоконно-оптичного зв'язку є безліч переваг перед іншими типами передачі інформації, такими як мідні жили і системи радіозв'язку.

Основні характеристики оптоволокна:

• Сигнал може бути переданий без регенерації на велику відстань (200 км).

• Оптоволоконна передача не чутлива до електромагнітних завад. Крім того, волокно не проводить електрику і фактично непомітно до радіочастотної інтерференції.

• Оптичні системи забезпечують більшу кількість каналів ніж фізичні ланцюга.

• Оптичний кабель набагато легше і тонше ніж кабель з металевими жилами і волокна займають в ньому невеликий обсяг. Наприклад, один оптоволоконний кабель може містити 144 волокна.

• Оптичне волокно дуже надійне [1].

Оптоволокно є практично ідеальним середовищем для передачі даних. Передача даних по ньому у вищій ступені безпечна, оскільки випромінювання зовні відсутнє, сигнали поширюються з меншим загасанням, отже, на великі відстані. Переданий сигнал складається з двох компонентів. Одним є посилається інформація, т. е. набір одиничок і нулів, а іншим - власне оптичний сигнал, який несе цю інформацію. Важливо розуміти, що ці компоненти реалізуються різними мережевими елементами, або рівнями. Перший відноситься до рівня синхронізації, тоді як другий - до оптичного. Серії з одиниць і нулів відповідають серія значень напруг, які згодом перетворюються в світлові імпульси, що випромінюються лазером [2].

Література:

1. *Принцип передачи світла по оптоволокну. http://izmer-ls.ru/w/o02.html*

2. Оптичні методи передачі даних в комунікаційних мережах. https://itc.ua/articles/opticheskie_metody_peredachi_dannyh_v_kommunikacionnyh_setyah_11461/

3. Оптоволокно: що воно собою представляє. https://f1comp.ru/internet/optovolokno-vs-vitaya-para-chto-vybrat-dlya-doma/#i-2

МУЛЬТИСЕРВІСНИЙ ДОСТУП В ІНТЕРНЕТ

Пелехай Сергій Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Мультисервісна мережа - це єдина мережа, здатна передавати голос, відеозображення і дані. Основним стимулом появи і розвитку мультисервісних мереж є прагнення зменшити вартість володіння, підтримати складні, насичені мультимедіа прикладні програми та розширити функціональні можливості мережевого обладнання [1].

Основними компонентами мультисервісних мереж є: телепорт, транспортна мережа та кластери.

Телепортом називається єдиний центр управління, отримання, обробки, створення і передачі інформації. Телепорт будується за модульною технологією (з можливістю поетапного нарощування послуг, що надаються) і формується з обладнання і програмного забезпечення (ПО) для організації прийому ефірних і супутникових ТВ- і радіопрограм;

Транспортна мережа - широкосмугова кабельна мережа, побудована за закрученою оптичною технологією зі структурою «Кільце» або «Зірка».

Кластери - це групи від 500 до 2 тисяч абонентів, територіально розташовані в безпосередній близькості один від одного і охоплюють розподільчу мережу.

Телепорт скріплює волоконно-оптичну транспортну мережу міських райських районів з найбільшою щільністю абонентів.

Мережі можуть поєднувати кабельну та бездротову технології, завдяки цьому мультисервісна мережа може виступати в ролі набору обладнання для створення, передачі, обробки та прийому інформаційних мереж для розподілу інформаційних потоків лінії, абонентське обладнання, а також набір послуг, що надаються споживачам.

Універсальність і модульність мультисервісної мережі дозволяє регулювати створений набір телекомунікаційних послуг, що надаються користувачам.

Доступ до Інтернету надає можливість обміну даними по мережі що дозволяє абонентам надавати високошвидкісний доступ (до 40 Мбіт / с) до Інтернету. Доступ до мережі може бути попередньо доставлений як індивідуальним абонентам, так і корпоративним, з можливістю гнучко регулювати пропускну здатність каналів передачі та різні версії трафіку. Для організації цієї послуги абонентам потрібен комп'ютер, за винятком кабельного модему, який встановлюється індивідуально або для групи абонентів. При відсутності у абонента персонального комп'ютера існує можливість підключення до Інтернету за допомогою кабелю до телевізійних станцій [2].

Література:

1. Мультисервисные сети. ***https://compress.ru/article.aspx?id=9404***

2. Multiservice Network. Network Elements.
http://www.telecomnetworks.ru/en/activities/systemintegration/ngn/mssystems/

5G МЕРЕЖІ

Подуран Давид Вадимович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Що таке 5G? Це нове покоління мобільного інтернету, яке має забезпечити значно швидшу передачу даних на телефон і з телефона, ширше покриття та більш стабільний зв'язок. Мова йде про досконаліше використанні радіо діапазону та можливості одночасного доступу до мобільного інтернету для більшої кількості пристроїв. Передбачено, що розгортання нових технологій відбуватиметься в декілька етапів. Спочатку буде впроваджено 5G NR Non stand-alone.

Зараз майже в будь-якій точці світу людина може поспілкуватися через інтернет за допомогою смартфона без підключення до локальної мережі або Wi-fi. Все це можливо лише за допомогою мобільного інтернету. Наразі існують мережі 2G, 3G, 4G та найновітніша 5G. Простою мовою — чим більше цифра, тим швидше і якісніше зв'язок.

В багатьох країнах зараз працює 4G, а подекуди є навіть 5G. Але в Україні якість мобільного інтернету покращилась лише кілька років тому, коли 3G замінила мережа 4G. Та вже наприкінці цього року влада планує почати впроваджувати ще більш швидкий інтернет — 5G. Крім швидкого інтернету нова технологія також дозволяє підключитися більшій кількості людей. Наприклад, якщо у вас на смартфоні ловить 4G, то до цього сигналу можуть приєднатися кілька тисяч приладів. До

сигналу 5G одночасно можуть підключитись до мільйона девайсів.

Завдяки швидкому мобільному інтернету, за словами представника Міністерства цифрової трансформації, вдасться покращити якість дистанційного навчання, а також внести різноманітність та цікавість до навчання за допомогою технологій. 5G забезпечить широкосмуговий зв'язок для підтримки додатків віртуальної та розширеної реальності, забезпечуючи дистанційне навчання та багатший навчальний досвід. Учні зможуть відвідати інші країни, планети або навіть здійснити екскурсію тілом людини завдяки віртуальній реальності (VR).

Системи бездротового зв'язку є предметом постійних досліджень і розробок як комерційними організаціями, так і в академічному світі. І як і будь-який тип зв'язку, вони повинні бути стандартизовані – їм повинен бути призначений певний діапазон характеристик електромагнітних хвиль, в яких мережа буде функціонувати. А також визначені всі вимоги і обмеження.

У разі систем радіозв'язку найбільш важливим міжнародним органом по стандартизації є консорціум 3GPP (Проект партнерства по мережах третього покоління), який, незважаючи на присутність в абревіатурі 3G (третє покоління), визначає стандарти і для наступних систем, в даний час – п'ятого покоління (5G). До консорціуму 3GPP входять сім національних і регіональних організацій зі стандартизації з різних частин світу (наприклад, ETSI – Європейський інститут стандартів електрозв'язку) і основні виробники телекомунікаційного обладнання.

Однією з технологій, яка буде використовуватися в мережах 5G, є NR – новий стандарт передачі даних, створений 3GPP. Ця ж організація відповідає за аналогічну технологію для мереж 4G під назвою LTE. Існує висока ймовірність того, що NR буде широко використовуватися по всьому світу. Організація 3GPP має сім так званих організаційних членів з Європи, Китаю, Японії, Південної Кореї. Перші смартфони, оснащені модемами 5G, вже з'являються на ринку, в тому числі в середньоціновому діапазоні. Проте, можливо, новий стандарт зв'язку стане популярним лише через кілька років. Експерти вважають, що цей період може затягнутися до п'яти років.

Література:

1. *https://root-nation.com/ua/articles-ua/tech-ua/ua-what-is-5g/*
2. *https://www.bbc.com/ukrainian/features-44934506*

ІНТЕРНЕТ-БАНКІНГ – ТЕЛЕКОМУНІКАЦІЙНИЙ ПРОРИВ

XXI СТОЛІТТЯ

Прокопенко Дмитро Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

У наш час важко уявити собі банк, у якого немає веб сторінки, або додатку для телефону. Будь які банки можуть використовувати їх як систему для онлайн операцій між картками та рахунками. Така система називається **інтернет-банкінгом**.

Інтернет-банкінг – це один із видів дистанційного банківського обслуговування, засобами якого є доступ до рахунків та операцій з ними в будь-який час та з будь-якого комп'ютеру через Інтернет. Інтернет-банкінг являється додатковим каналом обслуговування в банку, за допомогою якого можливо на відстані керувати своїми поточними та картковими рахунками, відкривати депозити, гасити кредити, здійснювати платежі та інші операції. Можна самостійно здійснювати більшість традиційних банківських операцій безперервно при наявності комп'ютера, ноутбука або смартфона із підключенням до Інтернету

На відміну від наших батьків, які були у нашому віці, зараз ми маємо змогу виконувати всі операції віддалено. Нам не потрібно їхати у відділення банку, щоб зробити платіж, ми можемо оплатити комуналку не виходячи з дому, та перевірити банківський рахунок, їхавши в метро.

У країнах Європи кількість банківських операцій у Інтернеті складає більше 30% від загального обсягу послуг. Кількість клієнтів інтернет-банкінгу у США та Європі вже досягла 120 млн. осіб., а оборот інтернет-банкінгу у Європі складає більше 5 млрд. євро.

Серед переваг інтернет банкінгу слід відзначити:

- дистанційне управління картою.
- швидке виконання фінансових операцій
- оплата послуг.
- взаємодія з банком.
- мінімальна або нульова комісія.

Але, як і у будь-якої телекомунікаційної системи, є мінуси. Вони не значні, але іноді можуть кидатися в очі. Серед них:

- ризик втрати грошей.
- ліміти.
- технічні збої.
- неможливість не взаємодіяти з банками взагалі.

Підведемо підсумки. Інтернет банкінг – це сучасна система, яка, не зважаючи на свої недоліки, допомагає людям швидше і продуктивніше робити банківські операції. Кількість людей що використовує послуги інтернет банкінгу зростає з кожною годиною і це один з найпоширеніших телекомунікаційних систем по всьому світу.

Література:

1. *http://oldconf.neasmo.org.ua/node/2772*
2. *spilnota.net.ua/ua/article/id-2908/*
3. *https://weekend.today/*

МЕТОДИКА ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ПІДСТАВІ ПРОТОКОЛУ MGCP

Рінсевич Володимир Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Об'єкт дослідження - мережі IP-Телефонії.

Мета роботи - дослідження принципів побудови мереж IP-телефонії на основі протоколів MGCP.

Метод роботи - виявлення можливостей практичного використання мереж IP-телефонії на основі протоколів MGCP.

Проведений аналіз можливостей мереж IP-телефонії на основі протоколу MGCP показав:

Принципи побудови мереж IP-телефонії дозволяють істотно скоротити смугу пропущення для передачі мови, відео й даних у режимі мультимедійних повідомлень і істотно знизити завдяки цьому вартість надаваних послуг абонентам. Сімейство протоколів H.323 забезпечує можливість передачі мовних повідомлень, відео й даних по мережах IP-телефонії й добре інтегрується з можливостями ТМЗК. Протокол MGCP є більш перспективним для побудови мереж IP-телефонії оскільки він побудований на декомпозиції транспортних шлюзів, що дозволяє скоротити час передавання сигнальних повідомлень.

Галузь використання – провайдерам Інтернет і операторам телефонного зв'язку введення IP-телефонії в спектр послуг відкриває зовсім нові ринки збуту, нових клієнтів і можливості розвитку. Корпоративним клієнтам і приватним користувачам - зниження витрат на міжміські (міжнародні) переговори, дзвінки з комп'ютера, дзвінки з Web-Сайту.

ВИСНОВКИ

Таким чином, в дипломній роботі викладені принципи побудови мереж IP-телефонії на підставі протоколу MGCP.

На основі проведеного вище порівняння можна зробити висновок, що для розгортання глобальних мереж IP-телефонії краще інших підходить протокол MGCP.

Розглянуто, що протокол SIP більше підходить для використання Internet-провайдерам, оскільки, в такому разі послуги IP-телефонії розглядаються лише як частина набору загальних послуг.

Відповідно, що оператори телефонного зв'язку, для яких послуги Internet не є першорядними, швидше за все, будуть орієнтуватися на протокол H.323, оскільки мережа, побудована на базі рекомендації H.323, представляється їм добре знайомою мережею ISDN, накладеною на IP-мережу.

Література:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2-е издание. – СПб.:Питер, 2005. – 864с.

СИСТЕМИ ГЛОБАЛЬНОГО ПОЗИЦІОНУВАННЯ

Родіонов Єгор Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Розглянуто для реалізації яких цілей було розроблено систему глобального позиціонування (GPS). Наведені переваги використання системи глобального позиціонування (GPS). Також розглянута сама побудова система глобального позиціонування (GPS) та сучасні компанії які уже на протязі довгого періоду, успішно розробляють апаратуру на основі технологій систем глобального позиціонування (GPS).

За останнє десятиліття системи глобального позиціонування завоювали величезну популярність. Нині у всьому світі розгорнуто чотири ГНСС, серед яких можна виділити *GPS* – Global Positioning System NAVSTAR розробленою Сполученими Штатами Америки.

Система GPS – це цифрова лінія зв'язку з кодовим розділенням, множинним доступом (CDMA). Супутникові сигнали складаються з синусоїдальної несучої, цифрового навігаційного повідомлення і послідовності псевдовипадкового шуму (PRN) з широкою смугою частот. Навігаційне повідомлення і послідовність PRN (код) кодуються в фазі несучого сигналу з використанням методу модуляції з двійковою фазовою маніпуляцією (BPSK).

Космічний сегмент сучасної системи містить 32 супутника системи NAVSTAR. Мінімально 24 супутника складають повне "сузір’я" супутників, що працюють в нормальному режимі на орбіті до кінця строку їх експлуатації. Знаходячись на орбіті, на

висоті 20200 км (велика напіввісь 26560 км) кожен супутник виконує за день два оберти навколо Землі (один оберт за 11 год 58 хв, швидкість обертання ≈ 3 км/с). Вони описують 6 орбітальних траєкторій, на кожній із яких знаходиться 4 і більше супутників. Завдяки цьому, в любій точці земного шару, протягом 24 годин будуть в межах прийому GPSприймача мінімум 4 супутника. Безперебійну працездатність системи забезпечують 24 супутника, проте, на випадок аварійних ситуацій і збоїв у роботі, загальна кількість супутників системи збільшена до 32.

Система GPS забезпечує 100% глобальну доступність навігаційних послуг на кутах місця вище 5 градусів. Середня точність навігації за рахунок самої системи (без урахування помилок приймального обладнання) становить близько 1 м. Відносна стійкість точних характеристик в системі GPS забезпечується за рахунок наземного комплексу управління з глобальним покриттям орбіт вимірювальними і закладними станціями. Крім того, в контурі управління реалізовані "індивідуальні" для кожного апарату типові цикли управління, що дозволяє оперативно реагувати на виникаючі відхилення в характеристиках того чи іншого космічного апарату.

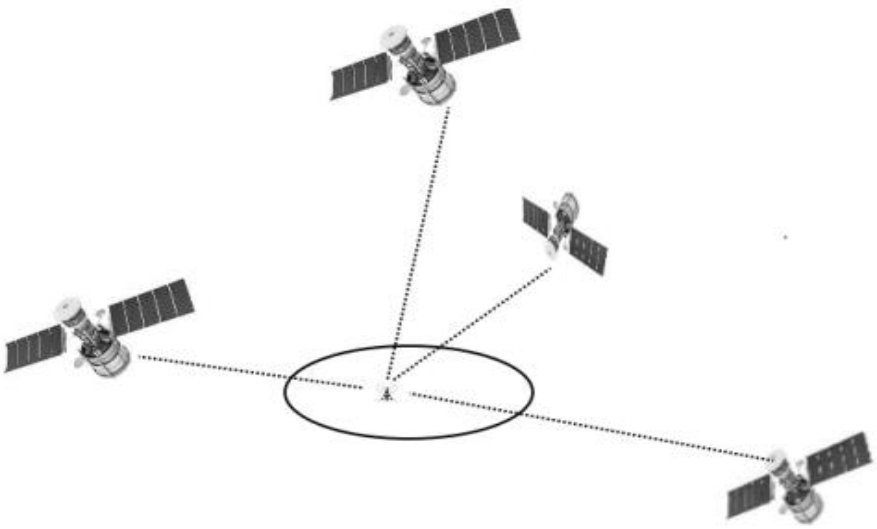


Рис. 1 Візуалізація роботи системи глобального позиціонування

Основним принципом використання системи є визначення місцерозташування шляхом вимірювання моментів часу прийому синхронізованого сигналу від навігаційних супутників антеною споживача.

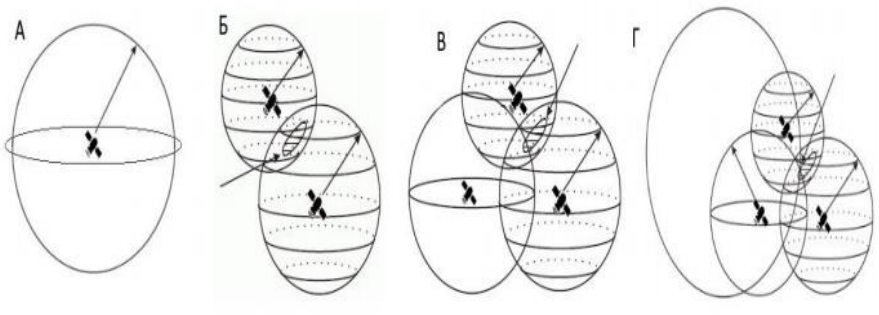


Рис. 1.1 Візуалізація накладання даних з сателітів

Визначення відстані до кожного супутника визначається по затримці передачі сигналу. Далі, отримавши просторові координати 3 точок і 3 відстаней до шуканої точки, знаходить місцезнаходження приймача на площині. Оскільки система супутникової навігації працює у просторі, а не на площині, то необхідна наявність четвертого супутника, котрий дозволяє однозначно визначити координати точки в тривимірному просторі. У порівнянні з рішенням теоретичного геометричного завдання, практичне визначення відрізняється ще й тим, що існують похибки визначення відстані до супутників, котрі призводять до того, що результатом визначення виявиться не певна точка, а область деякого радіуса, в якій знаходиться пристрій. Проте, збільшення кількості видимих супутників призведе до зменшення цього радіусу, а точність визначення місцерозташування зростає.

Література:

1. http://repository.vsau.org/getfile.php/24628.pdf

2. https://ela.kpi.ua/bitstream/123456789/23038/3/Sokolenko_magistr.pdf

SIP-ТЕЛЕФОНІЯ

Роздайбіда Владислав Дмитрович

Державний університет телекомунікацій

Навчально-науковий інститут Телекомунікацій

м. Київ

Найпопулярнішим типом фіксованого зв’язку є SIP-телефонія. Session Initiation Protocol - протокол ініціювання сеансу (SIP) - протокол передачі даних, дослівно перекладений як «протокол встановлення сеансу». Як і універсальна мова, він дозволяє пристроям обмінюватися даними та розуміти один одного без помилок.

SIP-телефонія працює, постійно змінюючи запити клієнтів та відповіді сервера постачальників. Крім SIP існують і інші

протоколи. Однак сьогодні Протокол ініціювання сесії є найбільш перспективним, універсальним та широко розповсюдженим стандартом обміну голосовими даними через Інтернет.

Почати варто з базового поняття - Інтернет-протокол (IP), або «міжмережний-протокол». Саме він з'єднав комп'ютерні мережі у всьому світі в одну глобальну мережу - Інтернет, використовуючи унікальну IP-адресу, призначену кожному пристрою, підключеному до Інтернету - комп'ютеру, ноутбуку, планшету або смартфону. IP-телефонія - загальна назва будь-якого комутованого з'єднання через Інтернет за допомогою мережевого протоколу IP. За допомогою цієї технології ви можете призначити номер телефону не певному місцезнаходженню, а конкретному користувачеві, який має доступ до мережі.

IP-телефонія є невід'ємною частиною VoIP (Voice over IP), технології передачі звукових даних по мережі. VoIP використовується не тільки для дзвінків через Інтернет, але і для передачі відео, конференцій, перегляду записів із камер відеоспостереження зі звуком тощо.

SIP-телефонія - один із протоколів зв'язку, що використовується в IP-телефонії, відрізняючись функціями та перевагами.

Для SIP-телефонії потрібно мінімум спеціального обладнання. Для користування послугою підходить будь-який із варіантів:

- настільний або портативний комп'ютер із попередньо встановленим програмним забезпеченням SIP-клієнта, гарнітурою та підключенням до Інтернету;
- оснащений планшетом або смартфоном із програмою SIP з доступом до мереж WI-FI, 3G або 4G;
- стаціонарний телефон SIP, який можна підключити до маршрутизатора;
- звичайний аналоговий телефон, підключений до шлюзу VoIP, який, у свою чергу, підключений до маршрутизатора.

Які рішення нам пропонує SIP-телефонія?

1. За необхідності ви можете швидко побудувати та розширити свою корпоративну телефонну мережу.

2. Дає можливість відповідати на дзвінки клієнтів в офісі, вдома або в дорозі. Досить встановити переадресацію дзвінка на мобільний телефон.

3. Спілкування стає зручним інструментом для спілкування з колегами та клієнтами, а також для аналізу ефективності компанії та контролю за роботою співробітників.

До основних переваг SIP-телефонії належать такі:

Доступність – міський номер працює скрізь, де є доступ до Інтернету зі швидкістю 64 Кбіт / с, не тільки вдома та в офісі.

Економія - номер SIP буде коштувати дешевше, ніж придбання, підключення та обслуговування дорогого обладнання для офісної АТС. Важливо, щоб можна було збільшити кількість користувачів або операторів корпоративних мереж без проблем і великих інвестицій.

Для роботи достатньо *простоти*: комп'ютер з гарнітурою та підключенням до Інтернету. Ця технологія також доступна на смартфонах, планшетах, ноутбуках, стаціонарних телефонах та SIP-телефонах.

Зручність - підключіть дані дзвінків до 1С, CRM, аналітичних систем та покращте ефективність вашого бізнесу. Створіть одну корпоративну телефонну мережу з нульовими тарифами. Налаштуйте один номер на кількох телефонах.

Універсальність - SIP-телефонія та відстеження дзвінків дозволяють відстежувати та контролювати навантаження відділу продажів, слухати дзвінки та перевіряти компетентність у роботі з клієнтом кожного спеціаліста. Ця технологія також підтримує багаторядкові номери і може використовуватися в АТС.

Гнучкість - ви можете створити унікальну схему перенаправлення між підрозділами та працівниками, яка підходить саме для вашої компанії. А також налаштуйте голосову пошту, автовідповідач, зручне голосове меню та зворотний дзвінок на веб-сайті.

Література:

1. Тарасов В. Ю., Дроздов К. И. Качество речи в IP-сетях [Электронный ресурс]. – Режим доступа: http://www.ccc.ru/magazine....

2. Макарова О. С. Способ оценки зависимости качества связи в системах IP-телефонии от критических параметров IP–сети // Молодой ученый. – 2011. – №12. Т.1. С. 83–86.

3. Гилазов М. Н. Влияние качества обслуживания на коммутацию IP-пакетов // Молодой ученый. – 2015. – №11. – С. 282–285.

INTERNET PROTOCOL VERSION 6

Роздайбіда Владислав Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

В 2012 році було запущено IPv6 - нову версію протоколу IP, яка замінила IPv4. Через стрімке зростання кількості смартфонів, планшетів та інших пристроїв, які можуть

підключатися до Інтернету, існує ризик того, що запас доступних IP-адрес скоро закінчиться. IPv6 вирішує цю проблему, а також кілька інших вразливих місць безпеки.

Протокол мережевої взаємодії TCP / IPv4 використовується для передачі зашифрованих даних через Інтернет та локальні підмережі вже більше тридцяти років. На його основі створюється та підтримується унікальна адресація мережевого обладнання (вузлів). Вже на початку 1990-х був визначений головний недолік цього протоколу - обмеження кількості можливих IP-адрес, яке не може перевищувати 4,23 млрд.

Результатом стала нова система для запису мережевих взаємодій - Інтернет-протокол версії 6. Однак масовий перехід до більш досконалих технологій обумовлений деякими труднощами. Хоча, наприклад, у США більше половини користувачів уже використовують протокол IPv6.

На жаль, IPv4 та IPv6 несумісні, тому існує потреба в поступовому переміщенні Інтернету з однієї версії протоколу на іншу. Існують різні методи переходу. Найбільш поширеним рішенням є призначення IPv4 і IPv6 адрес, поки більша частина Інтернету не перейде на IPv6.

Порівняно з четвертою версією, TCP / IPv6 реалізує багато інших функцій:

- використовуються простіші заголовки для виключення нерелевантних параметрів, тим самим зменшуючи навантаження на маршрутизатори при обробці мережевих запитів;
- вищий рівень безпеки, автентифікації та конфіденційності є основою цієї технології;
- протокол реалізує функцію якості обслуговування (QoS), яка дозволяє визначати чутливі до затримки пакети;
- використовувати групи багатоадресної передачі при передачі широкомовних пакетів;
- для підвищення безпеки використовується підтримка стандарту шифрування IPsec, який дозволяє шифрувати дані без будь-якої підтримки прикладного програмного забезпечення.

Звідси виникає запитання: якщо TCP / IPv6 має стільки переваг перед своїм попередником, чому б просто не перейти на нього у глобальному масштабі?

Основна причина - вартість. Оновлення всіх серверів, маршрутизаторів і комутаторів, які завжди покладались на IPv4, вимагає багато грошей і часу. Крім того, для вирішення проблеми недостатньої кількості адрес провайдер призначить користувачеві динамічну адресу, яка зміниться при підключенні

до іншої мережі. Після від'єднання від мережі пристрій звільнить свою адресу, зробивши доступною для інших пристроїв. Насправді ви знімаєте будинок, але у вас немає адреси. Це значно уповільнило перехід від IPv4 до IPv6.

Але це не означає, що IPv6 не поширюватиметься. Натомість він використовується паралельно з IPv4. За даними Google, близько 14% користувачів використовують IPv6. За даними Comcast, половина користувачів у США вже використовує IPv6.

Справа не в тому, що IPv6 швидший і безпечніший, але він має багато переваг, таких як більш ефективна маршрутизація без фрагментації пакетів, вбудована підтримка IPsec та автоматичне налаштування адреси. І через обмежений адресний простір IPv4 перехід на нього неминучий.

Література:

1. Гольдштейн Б. С., Соколов Н.А., Яновский Г. Г. Сети связи. СПб.: БХВПетербург, 2010.

2. J. Jeong; S. Park; L. Beloeil; S. Madanapalli (November 2010) IPv6 Router Advertisement Options for DNS Configuration - tools.ietf.org/html/rfc6106.html, IETF. RFC 6106.

РОЗРОБКА ПРОЕКТУ МАГІСТРАЛЬНОЇ ВОЛЗ МІЖ НАСЕЛЕНИМИ ПУНКТАМИ ВІННИЦЯ-ПОЛТАВА

Савченко Богдан Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Об'єкт дослідження – Розробка проекту магістральної ВОЛЗ між населеними пунктами Вінниця-Полтава.

Предмет дослідження – Методи моніторингу в системах DWDM.

Мета роботи – Прокладка ВОЛЗ між населеними пунктами Вінниця – Полтава.

Методи дослідження – теорії електрозв'язку, теоретичної радіотехніки, математичного та комп'ютерного імітаційного моделювання.

В роботі приведено основні відомості про системи та мережі дротового зв'язку та виявлено тенденції їх сучасного розвитку. Сформульовано нові задачі підвищення їх ефективності як на етапі аналізу окремих функціональних вузлів так і синтезу системи та дротової мережі в цілому за технічними вимогами. Проведена оцінка пропускної спроможності мережі з високою інтенсивністю передачі інформації.

ВИСНОВКИ

В результаті виконання магістерської кваліфікаційної роботи досліджено параметри оптичного волокна. Можуть бути різні варіанти побудови конкретних систем, що відрізняються ступенем захисту і контролю несанкціонованого доступу до інформації, що передається по ВОЛЗ інформації. Це робить необхідним проведення спеціальних досліджень з метою експертизи реалізованих науково-технічних рішень та їх відповідності вимогам забезпечення захисту інформації. Тому важливою проблемою в області захисту ВОЛЗ є розробка нормативної та методичної бази і документів, що забезпечують і регламентують як розробку захищених ВОЛЗ,так і порядок їх впровадження в мережах зв'язку. Ця проблема вимагає свого прискореного вирішення.

Тут необхідно зазначити, що всі перераховані вище методи захисту і їх комбінації можуть забезпечувати безпеку інформації лише в рамках відомих моделей загроз нападу. При цьому ефективність систем захисту визначається як відкриттям нових, так і вдосконаленням технологій застосування вже відомих фізичних явищ. З плином часу противник може освоїти нові методи перехоплення, буде потрібно доповнювати захист, що не властиво криптографічним методам захисту, які розраховуються на досить тривалий термін. Тому, завжди актуальний захист саме від не санкціонованого доступу до волокон но-оптичних ліній зв'язку, а саме, до місць прокладки кабелів.

Література:

1. Посібник ''Оптов-олоконних мереж'' https://deepnet.ua/uchebnik- volokonno-opticheskie-seti.html

2. Телекомунікаційне обладнання https://www.optokon.ua/

СПОЧАТКУ БУЛО СЛОВО… А ПОТІМ АУДІО-КОДЕК

Свердлюк Боглан Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Звук… Увесь звук, що ми маємо, ми можемо умовно розділити на два типи. Аналоговий звук. Такий звук ви чуєте в старому дисковому телефоні, а зберігається він на таких носіях, як венил, плівка, чи щось старіше, наприклад воскова трубочка Едісона. І цифровий звук. Це ваша улюблена пісня, чи радіо програма. Він може зберігатись на цифрових носіях. Власне від того і головний мінус аналогового звуку. Він програє в відношенні перезапису і багаторазового відтворення. Як би там не було цифровий звук надовго ввійшов у наш побут. В тому числі і в телефонію.

У традиційній телефонії установка з'єднання відбувається за допомогою телефонної станції, у разі ж IP-телефонії, стислі пакети даних поступають в глобальну або локальну мережу з певною адресою. При цьому IP-телефонія виявляється дешевшим рішенням як для оператора, так і для абонента. Разом з тим, IP-телефонія дозволяє поліпшити якість зв'язку.

Звук та цифра

Аналоговий сигнал - це безперервний у часі сигнал. Він має недоліки в записі, копіюванні та відтворювані звуку. Саме по цим причинам частіше всього використовується цифровий сигнал.

Цифровий звук

Перетворення аналогового сигналу в цифровий складається з двох частин: дискретизацією по часу, та квантування по амплітуді. Дискретизацією по часу, вказує, що сигнал представляється рядом звітів -sample, взятих через певний проміжок часу. беруть і записують координати графіка.

Звук є функція від часу, тому точки на осі вибирають з певним інтервалом, або з певною частотою - це називається частотою дискретизацією. А ось амплітуду потрібно розбити на певну кількість значень, яка буде достатньою, щоб відновити наш сигнал з достатньою точністю, ця кількість називається глибиною квантування, її виміряють в бітах. 1=2 значенням на амплітуді. Для передачі мови і її точного відновлення на стороні отримувача вистачає 12 біт, для запису пісень 16 біт. Тепер потрібно зрозуміти, як багато повинно бути звітів?

Теорема Котельникова (Найквіста - Шеннона)

Будь-яку функцію часу, яка складається від 0 до f можна передавати безперервно з будь якою точність за допомогою чисел, які йдуть один за одним через 1/2f сек. Тобто, для того, щоб точно відновити сигнал на стороні приймача, його частота має бути вдвоє більша заданої. Оскільки людський слух сприймає діапазон частот від 16 гц до 20 Кгц, дослідами було виявлено, що оптимальний канал для передачі телефонного сигналу складає 30 -3400 КГц. Меншу частоту дискретизації обирають для зменшення розміру файлу, наприклад в військових структурах з металізованим голосом

Є ще один параметр, який впливає на якість звуку, це швидкість передачі звуку - бітрейт. Чим більше інформації. тим швидше його потрібно передати. Для мінімальних показників, тобто для 44,1 Кц і 16 біт без втрати якості потрібний канал звязку 1411,2 кб.с.

<u>Трохи теорії</u>

Компандування

Компандування (від англ. Companding - compression + expanding) - це метод зменшення ефектів каналів з обмеженим динамічним діапазоном. Заснований на збільшенні числа інтервалів квантування в області малих значень вхідного сигналу і зменшенні в області максимальних значень.

Затримка - затримка звуку за рахунок передачі, кодування та розкодування аудіопотоку.

Дискретизація - це процес перетворення будь-якого вибіркового аналогового значення у відповідне дискретне значення, до якого може бути присвоєно унікальне цифрове кодове слово.

PCM - це метод кодування за формою сигналу, заданий в специфікації ITU-T G.711.

Кадр - Обмін інформацією проводиться кадрами; за допомогою тимчасового поділу в кожному кадрі. Кожен кадр тривалістю 10 мс розділений на 24 тимчасових інтервали (або англ. Slot), причому перші 12 тимчасових інтервалів (0-11) служать для передачі пакетів в напрямку отримувача, а наступні 12 (12-23) для передачі пакетів в зворотному напрямку

MIPS - одиниця вимірювання швидкодії, що дорівнює одному мільйону інструкцій у секунду. Якщо зазначено швидкодію в MIPS то, як правило, вона показує, скільки мільйонів інструкцій на секунду виконує процесор в деяких синтетичних тестах.

Кодек

Усі кодеки також умовно можна розділити на два види: кодеки загального призначення (великі затримки, висока якість), та кодування мовлення (низька якість, маленькі затримки). В даній статті я розглядаю варіант №2.

Передача звуку в незжатому вигляді дуже рідке явище. Більшість кодеків використовують зжимання файлу з втратою якості, але це не є проблемою, оскільки зміни для людського слуху не помітні. Така втрата може зменшувати аудіо файл у декілька разів.

G.711 Для того, щоб оцифрувати аналоговий сигнал потрібно, виконати квантування сигналу по рівню від -127 до 127. Таким чином, кожен звіт буде дорівнювати 1 байту. В данному випадку максимальною частотою вважається 4 000 Гц, згідно теоремі помножимо його вдвічі та отримаємо 8 000 звітів та пропускну здатність каналу 64 Кбіт/с

G.729 На відміну від попереднього кодек G.729 передає тільки рівень зміни звіту по зрівнянню з попереднім, а також використовує кодову книгу. Тому цей кодек в 8 разів ефективніше за попередній.

G.723.1 6.4 Кбіт / с (кадр має розмір 189 бітів, доповнених до 24 байтів) і 5,3 Кбіт / с (кадр має розмір 158 бітів, доповнених до 20 байтів). Режим роботи може змінюватися динамічно від кадру до кадру.

G.726 - використовує кодування мови на основі алгоритму Adaptive Differential Pulse Code Modulation (ADPCM).

Основне його використання - це інтернаціональні канали зв'язку з економією смуги пропускання. Якщо G.711 використовує смугу в 64 Kbps, то G.726 використовує 32 Kbps, забезпечуючи приблизно таку ж якість зв'язку.

G728 Кодек G.728 використовує оригінальну технологію з малою затримкою LD-CELP (low delay code excited linear prediction) Даний кодек спеціально розроблявся для ущільнення телефонних каналів, при цьому було необхідно забезпечити дуже малу величину затримки (менше 5 мс). Кодер має тривалість кадру тільки 0.625 мс. Реально затримка може досягати 2.5 мс. Недоліком алгоритму є висока складність - близько 20 MIPS для кодера і 13 MIPS для декодера - і відносно висока чутливість до втрат кадрів.

G.729A Кодек G.729 дуже популярний в додатках передачі мови по мережах Frame Relay. Кодек використовує кадр тривалістю 10 мс і забезпечує швидкість передачі 8 Кбіт / с. Для кодера необхідний попередній аналіз сигналу тривалістю 5 мс.

Існують два варіанти кодека:

• G.729, що вимагає близько 20 MIPS для кодера і 3 MIPS для декодера.

• Спрощений варіант G.729A, що вимагає близько 10.5 MIPS для реалізації кодера і близько 2 MIPS для декодера.

Opus

Цей кодек володіє достатньою гнучкістю, щоб підтримувати кодування звуку будь-якого виду, як в максимальній якості, так і з маленькими затримками.

Тести підтверджують:

На 64 кбіт / с Opus звучить краще, ніж HE-AAC або Vorbis

На 64 кбіт / с Opus звучить так само, як 96 кбіт / с MP3

Opus одночасно добре підходить і для трансляції музики на 6 кбіт / с і на 256 кбіт / с, при цьому на широкій смузі Opus забезпечує стиск «без сприймається на слух» втрати якості. Кодек може динамічно перемикатися на стиск з різним бітрейтом, в залежності від зміни умов смуги пропускання.

iLBC

Кодек iLBC (Internet Low Bitrate Codec) поєднує в собі низьке використання смуги пропускання і високої якості. Даний кодек ідеально підходить для підтримки високої якості зв'язку в

мережах з втратами пакетів. iLBC не такий популярний як кодеки стандартів ITU і тому, може бути несумісний з популярними IP - телефонами і IP - ATC.Internet Low Bitrate кодек використовує складні алгоритми для досягнення високого показника стиснення, тому, досить відчутно завантажує процесор. На даний момент iLBC використовується безкоштовно, але власник цього кодека, Global IP Sound (GIPS), зобов'язує повідомляти користувачів про намір комерційного використання цього кодека. Кодек iLBC працює на швидкості в 13.3 Кб / сек. з фреймами в 30 мс, і на швидкості 15.2 кб / сек. з фреймами в 20 мс.

Speex

Кодек Speex відноситься до сімейства кодеків змінної швидкості (variable-bitrate, VBR), що означає можливість кодека динамічно змінювати швидкість передачі бітів в залежності від статусу продуктивності мережі передачі. Цей кодек пропонується в широкосмугових і вузькосмугових модифікаціях, в залежності від вимоги до якості. Speex повністю безкоштовний і поширюється під програмної ліцензією університету Берклі (Berkeley Software Distribution license, BSD). Кодек працює на діапазонах від 2.15 до 22.4 Кб / сек. в рамках змінного бітрейта.

GSM

Кодек для глобального стандарту цифрового мобільного стільникового зв'язку (Global System for Mobile Communications, GSM) не обтяжений ліцензуванням, як його аналог G.729A, але пропонує високу якість і помірну навантаження на процесор при використанні 13 Кб / сек. смуги пропускання. Експерти вважають, що якість GSM трохи нижче ніж G.729A.

LPC10

LPC - англ. Linear Predictive Coding - лінійне кодування з пророкуванням. LPC10 використовується для ліній зв'язку з вузькою пропускною спроможністю з бітрейтом 2.5 Кбіт / с. Голосовий сигнал чистий, але звучання схоже на голос робота.

GIPS

GIPS (Global IP Sound) - виробник сімейства кодеків VOIP і відповідного програмного забезпечення. Його швидкість передачі становить: 13,3 кб / с і вище. Кодек GIPS може підтримувати якість передачі голосу з 30% втратою пакетів. Дана технологія є ліцензованою для використання Skype.

GIPS створили iLBC вузькосмугового кодека, який вони також надають, однак під обмеженою, але вільною ліцензією. Такий кодек за замовчуванням підтримується в Asterisk і є стандартом IETF.

AMR Codec

AMR (англ. - Adaptive Multi-Rate) кодек дозволяє декодувати вузькосмугові сигнали (200-3400Гц) при змінному бітрейті в діапазоні від 4,75 до 12,2 кбіт з якістю, починаючи з 7,4 кбіт для міжміських дзвінків. Кодек AMR - стандартний кодек, обов'язковий для 2.5G / 3G бездротових мереж, який працює на базі GSM (WDMA, EDGE, GPRS).

Отже, з кожним роком розроблюються нові стандарти аудіокодеків. Вдалий тому приклад - Opus. Прийоми, що використовують такі кодеки дозволяю зробити зв'язок якіснішим, не перенавантажуючи канал інформацією, що в свою чергу може вплинути і на меншу ціну послуги в подальшому.

Література:

1. *bit.ly/2iV9iAU*
2. *habrahabr.ru*
3. *bit.ly/2nBkuo2*
4. *opus-codec.org*
5. *youtu.be/GPLXtqoYFzq*
6. *youtu.be/0CEeJkJYeAs*
7. *wiki.merionet.ru*
8. *terratel.eu/ru/voip-codecs*

СИСТЕМА «РОЗУМНИЙ БУДИНОК»: ВИСОКОІНТЕЛЕКТУАЛЬНЕ ЖИТЛО

Свиридов Дмитро Олексійович

Державний університет телекомунікацій

Навчально-науковий інститут Телекомунікацій

м. Київ

Будинок, в якому самі по собі відкриваються двері, включаються побутові прилади, регулюється температура і засуваються жалюзі, схожий на кадр з фільму про далеке майбутнє. Однак майбутнє набагато ближче, ніж нам здається. Система «розумний будинок» дозволяє повною мірою відчути блага технічного прогресу і позбавляє людину від вирішення безлічі побутових завдань.

Що таке «розумний будинок»?

Вперше поняття «розумний будинок» з'явилося в 50-х роках минулого століття. Прародителькою системи, здатної контролювати обстановку в цілому будинку, є технологія Java. Розробники цієї технології намагалися впровадити її в побутові прилади, тим самим зробивши їх більш «інтелектуальними».

Наприклад, вже в той час почали з'являтися перші вбудовувані мікрохвильові печі, кондиціонери, здатні регулювати мікроклімат приміщення залежно від погоди за вікном і т. д.

Однак поняття «розумний будинок» включає в себе не тільки інтелектуальну побутову техніку. Якщо пояснювати

простими словами, то ця система координує роботу всіх технічних пристроїв, що знаходяться в будинку. Причому управління системою може здійснюватися як за допомогою пульта, так і дистанційно, за допомогою сучасних девайсів — айфона, смартфона, планшета і т. д.

Можливості системи «розумний будинок» воістину багатогранні. Наприклад, щоб запобігти ймовірність пограбування, коли в будинку нікого немає, система імітує присутність господаря шляхом раздвигания жалюзі, включення/вимикання світла і т. д. Якщо ж зловмисники все ж проникають всередину приміщення чи відбувається інша екстраординарна ситуація, система миттєво сповіщає про це господаря. Крім того, технологія «розумний будинок» дозволяє структурувати роботу всього технічного та інженерного обладнання, задавши йому певний сценарій. Наприклад, перед вашим пробудженням система нагріє підлоги у ванній кімнаті, включить музичний центр, налаштує роботу кондиціонера на задану температуру, відрегулює оптимальну вологість в приміщенні і вирішить безліч інших побутових завдань.

Що включає в себе розумний будинок?

Отже, повноцінна система "Розумний дім" об'єднує в собі наступні вузли пристроїв:

- пристрої, що відповідають за захист від пожеж, а також охоронна сигналізація;
- апарати, контролюючі газо - і водопостачання;
- пристрої, що відповідають за охолодження і вентиляцію повітря;
- устаткування, що контролює подачу електричної енергії та опалення;
- пристрої, які контролюють побутову техніку, встановлену в оселі.

Установка системи «розумний будинок»

В ідеалі, монтаж бездротової системи «розумний будинок» має здійснюватися на етапі планування об’єкта. Однак деякі елементи системи можна безперешкодно встановити і в готовому будинку або квартирі.

Перед установкою системи спільно з фахівцем потрібно визначити кілька важливих нюансів:

- всі приміщення будинку будуть підключені до технології;
- де будуть розміщені відеокамери;
- будуть вони прихованими чи ні;
- як буде розташована схема освітлення;
- де будуть розташовані протипожежні датчики;

- які деталі об’єкта потраплять під управління і т. д.

Після визначення всіх аспектів роботи системи можна переходити до вибору обладнання для «розумного будинку», яке, залежно від типу роботи, може бути дротових або бездротових.

Оскільки процес установки системи «розумний будинок» досить складний і трудомісткий, провести його без допомоги фахівця неможливо.

Система «розумний будинок» робить житло максимально зручним, комфортним і безпечним. Завдяки технічній досконалості, вона значно спрощує життя людини, економлячи при цьому час і енергетичні ресурси.

Висновки

Скажи мені, де ти живеш, і я скажу тобі, хто ти. Саме так можна перефразувати стародавній вислів. Адже будинок - це спосіб виразити себе. Хочете, щоб ваш будинок був не тільки красивим і затишним, а й «відрізнявся розумом і кмітливістю»? Щоб можна було забути про N-нное кількість пультів, які розкидані по всьому будинку і їх ніколи не знайдеш. Щоб можна було керувати будь-яким приладом в будинку, освітленням, приймати повідомлення, спілкуватися з прийшли гостями, не встаючи з дивана. У «розумному» будинку все це вам під силу. Ваш будинок повністю підкоряється вам і вашим бажанням.

Література:

1. *http://bud-porada.in.ua/sistema-umnyj-dom.htm*
2. *http://yakrobitiremont.pp.ua/sistema-rozumnij-budinok-visokointelektualne-zhitlo/*

ІННОВАЦІЙНИЙ СТАНДАРТ БЕЗДРОТОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ WI-FI 6E

Слободян Олександр Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Протягом 2020 року на ринку було все легше знайти Wi-Fi 6-сумісні пристрої: стандарт 802.11ax повністю визначений, і в повній мірі використовується, як того вимагає Wi-Fi Alliance. Тим часом, зараз, коли більшість все ще використовує з'єднання Wi-Fi 5 (стандарт 802.11ac), вже визначено новий стандарт Wi-Fi - Wi-Fi 6e.

На відміну від звичайного Wi-Fi 6, стандарт Wi-Fi 6E використовує не тільки стандартні частоти 2,4 і 5 ГГц, а й нову частоту 6 ГГц, що в свою чергу розширює можливості і швидкості передачі данних. Основна перевага роботи на 6 ГГц є більше число каналів всередині частоти. Так, заявляється, що в Wi-Fi 6E буде 14 додаткових каналів на 80 МГц і 7 додаткових

каналів на 160 МГц. Це, в теорії, дозволить знизити рівень шуму для окремого пристрою та поліпшити користувальницький досвід користування бездротовими мережами в місцях високої щільності точок доступу.

Оскільки раніше частота 6 ГГц використовувалась дуже обмежено і в основному для військових цілей, з приходом нової технології деякі країни відкрили ділянки спектру в діапазоні 6 ГГц для неліцензійного використання. Це найбільше доповнення спектра за останні 20 років, оскільки FCC проклав шлях для Wi-Fi ще в 1989 році, тому це величезна подія для інформаційних мереж. Новий спектр в основному збільшує в чотири рази простір, доступний для маршрутизаторів та інших пристроїв, тому це буде означати набагато більшу пропускну здібність та набагато менші перешкоди для будь-якого пристрою, який може цим скористатися.

Мережі Wi-Fi мають великий вплив в повсякденному житті, однак попередні версії стандарту, аж до Wi-Fi 5, мали ряд архітектурних обмежень, які серйозно впливали як на якість з'єднання, так і на його швидкість.

Тільки в Wi-Fi 6, продовженням якого є Wi-Fi 6E, було реалізовано умовне «туннелирование» кількох пристроїв на різні антени роутера. На більш ранніх версіях протоколу кілька підключених пристроїв до однієї точки не могли звертатися до неї одночасно. Wi-Fi 6 за рахунок розподілу підключень по конкретним каналам і антен здатний забезпечити постійне підключення відразу для декількох девайсів, а розмежування їх по різних каналах всередині робочого діапазону дозволяє знизити рівень шуму між девайсами.

Wi-Fi 6E може все те ж саме і навіть більше: якщо попередня версія протоколу працює на частотах 2,4 ГГц і 5 ГГц, то в Wi-Fi 6E додаються частоти більшої пропускної здатності діапазону 6 ГГц, при цьому зберігається як можливість розмежування пристроїв по різних частотах і каналах, так і переключення їх на різні антени. Само собою, новий діапазон зацікавить жителів багатоквартирних будинків, в яких рівень шуму на частотах 2,4 ГГц можна назвати позамежним, а діапазон 5 ГГц вже досить серйозно навантажений.

Література:

1. https://ru.wikipedia.org/wiki/IEEE_802.11ax

2. https://www.theverge.com/2020/4/23/21231623/6ghz-wifi-6e-explained-speed-availability-fcc-approval

РОЗРОБКА ПРОЕКТУ ДІЛЬНИЦІ МАГІСТРАЛЬНОЇ ВОЛЗ МІЖ НАСЕЛЕНИМИ ПУНКТАМИ МУКАЧЕВО - СУМИ

Тертичний Роман Миколайович

Державний університет телекомунікацій

Навчально-науковий інститут Телекомунікацій
м. Київ

Поява оптичного волокна спричинила величезний прорив у розвитку сучасних телекомунікацій. Стрімкий розвиток ринку телекомунікацій призвів до доступності інформаційних послуг, а збільшення інформатизації суспільства спричинило значний приріст попиту, який й досі не зменшується, але навпаки, зростає з кожним роком в арифметичній прогресії.

Зважаючи на вищевказані обставини потрібно підвищувати рівень конкуренції шляхом впровадження нових магістральних волоконно-оптичних ліній зв'язку та модернізації старих.

Об'єкт дослідження – розробка проекту магістральної ВОЛЗ між населеними пунктами Мукачево - Суми.

Предмет дослідження – магістральна ВОЛЗ між населеними пунктами Мукачево - Суми.

Мета роботи– розробити проект магістральної ВОЛЗ між населеними пунктами Мукачево - Суми.

Методи дослідження – розрахункова робота, нормативна документація, аналіз обладнання на ринку телекомунікацій у галузі магістральних мереж.

В роботі приведено основні відомості про волоконно – оптичні магістральні мережі світу та України. Тенденції їх сучасного розвитку. Сформульовано нові задачі підвищення їх ефективності, та запропоновано методи їх вирішення. Проаналізовано різні методипідвищення ефективності магістральних ВОЛЗ, та розроблено один з них на базі магістральних ВОЛЗ між населеними пунктами Мукачево – Суми.

Висновки

1. В процесі виконання роботи був вибраний тип оптичного волокна, а також проведений розрахунок довжини ділянки регенерації.

2. У магістральних ВОЛЗ витрати на придбання та прокладку кабелю є основною частиною вартості всієї системи. Тому доцільно прокласти кабель з можливо низьким загасанням і широкою смугою частот в розрахунку на можливість його використання при розвитку системи.

3. На основі завдання було розраховано пропускну здатність та обраний необхідний тип оптичного кабелю.

Література:

1. Посібник ''Оптов-олоконних мереж''https://deepnet.ua/uchebnik- volokonno-opticheskie-seti.html

2. Телекомунікаційне обладнання https://www.optokon.ua/

ТЕЛЕКОМУНІКАЦІЇ

Тонкий Ілля Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі. Ознайомити слухачів з терміном телекомунікації та цікавими фактами.

Мета дослідження. Донести інформацію про телекомунікації:

1. Що таке телекомунікації?
2. Шлях людства до телекомунікацій.

Результати дослідження.

Телекомунікації - це передавання та приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду дротовими, радіо, оптичними або іншими електромагнітними системами. Телекомунікація виникає при обміні інформацією між учасниками з використанням технологій. Передача відбувається або за допомогою електрики, що проходить через фізичні носії, як кабель, або за допомогою електромагнітного випромінювання. Зазвичай, шляхи передачі розділяють на канали зв'язку, що дозволяє користуватись перевагами мультиплексування. Термін часто використовується в множині, тобто телекомунікації, тому що для передачі використовуються багато різних технологій.

Свійські голуби використовувалися в протягом століть різними культурами. Голубина пошта має перське коріння і використовувалася римлянами у військових цілях. Фронтін говорив, що Юлій Цезар використовував голубів для передачі повідомлень під час завоювання Галлії. Греки також пересилали повідомлення з іменами переможців Олімпійських ігор до різних міст використовуючи свійських голубів.

На початку 19-го століття, голландський уряд користувався таким рішенням на Яві та Суматрі. А у 1849 році, Поль Рейтер відкрив голубину пошту, яка передавала біржові ціни між Аахеном та Брюсселем, та працювала протягом року, доки не була замінена телеграфом. У середні віки, ланцюги маяків широко використовувалися на верхівках гір як засіб передачі сигналу. Основний недолік маякових ланцюгів полягав у тому, що вони могли передати лише один біт інформації, тому значення повідомлення, як-от «виявлено ворога» слід було узгодити заздалегідь. Одним з помітних прикладів їх

використання було протягом Іспанської Армади, коли маякові ланцюги передали сигнал з Плімута в Лондон.

У 1792 році, французький інженер Клод Шапе створив першу фіксовану систему телеграфу між Ліллем та Парижем. Однак, недоліком оптичних телеграфів була необхідність у кваліфікованих операторах та дорогих вежах на відстані до тридцяти кілометрів одна від одної. В результаті конкуренції з електричним телеграфом, остання комерційна лінія була покинута у 1880 році. Сір Чарльз Вітстон та сір Вільям Кук винайшли електричний телеграф у 1837 році. Також, перший комерційний електричний телеграф мабуть, був побудований Вітстоном та Куком та відкритий 9 квітня 1839 року. Обидва винахідники розглядали іхній пристрій, як «поліпшення електромагнітного телеграфу», а не як новий пристрій.

Самюел Морзе незалежно розробляв версію електричного телеграфу, який він безуспішно продемонстрував 2 вересня 1837 року. Його код був важливою перевагою у порівнянні з методом передачі Вітстона. Перший трансатлантичний телеграфний кабель було успішно прокладено 27 липня 1866, що дозволило вперше здійснити трансатлантичну телекомунікацію. Стаціонарний телефон був винайдений незалежно один від одного Алекстандром Беллом та Елішем Грей у 1876.

Антоніо Меуччі винайшов перший пристрій, який дозволяв електричну передачу голосу кабелем у 1849 році. Однак, його пристрій мав мале практичне значення, оскільки він був оснований на електрофонічному ефекті і тому вимагав, щоб користувачі розміщували приймач у своєму роті, щоб «чути» те, що було сказано. Перший комерційні телефонні послуги були встановлені у 1878 та 1879 по обидва боки Атлантики в містах Нью-Хейвей та Лондон. У 1832 році Джеймс Ліндсі продемонстрував бездротовий телеграф його студентам. До 1854 року, він зміг продемонструвати передачу через Ферт Тай з Данді, Шотландія до Вудхейвен, що на відстані трьох кілометрів, використовуючи воду як джерело передачі.

У грудні 1901 року, Гульєльмо Марконі встановив бездротове з'єднання між Сент-Джонсом та Полдху, за що отримав у 1909 році Нобелівську премію у фізиці. Проте, невеликий радіозв'язок вже продемонстрував в 1893 році Нікола Тесла на презентації Національної асоціації електричного світла. 25 березня 1925 року, Джон Бейрд зумів продемонструвати передачу рухомого зображення у лондонському універмазі Селфріджез. Пристрій Бейрда буз заснований на диску Ніпкова і став відомим як механічне телебачення. Він став основою експериментальних трансляцій, зроблених Британською

телерадіомовною корпорацією починаючи з 30 вересня 1929 року.

Проте у більшості телевізорів 20-го століття використовувалась електронно-променева трубка, яку винайшов Карл Браун. Першу версію такого телевізора було зроблено Філом Фарнсуртом, який показав його сім'ї 7 вересня 1927 року. 11 вересня 1940 року Джордж Стібіц передав задачу для свого калькулятора комплексних чисел у Нью-Йорку за допомогою телетайпу та отримав результат обчислень у Дартмутському коледжі в Нью-Гемпширі.

Така конфігурація централізованого комп'ютера (мейнфрейму) з терміналами віддаленого доступу залишалася популярною і в 1970-х. Проте вже в 1960-х роках дослідники почали розробляти пакетну передачу, технологію, яка посилає повідомлення асинхронно і по частинах до місця призначення, не передаючи його через централізований мейнфрейм. Мережа, яка складалася з чотирьох вузлів, виникла 5 грудня 1969 року, що є датою початку роботи ARPANET, яка до 1981 року зросла до 213 вузлів. ARPANET зрештою об'єднався з іншими мережами для формування Інтернету. Хоча завдання розробки Інтернету було зосереджено на Робочій Групі Інженерної Мережі Інтернету (IETF), яка опублікувала серію документів для запиту коментарів, інші розробки мережі відбувалися в промислових лабораторіях, як-от розробка локальної мережі (LAN) Ethernet (1983 р.) та протоколу token ring (1984 р.)

Стрімкий розвиток бездротових мереж почався в 1990-х роках, коли поява цифрових бездротових мереж призвела до соціальної революції та переходу парадигми від дротових технологій до бездротових, включаючи поширення комерційних технологій, як-от мобільні телефони, мобільна телефонія, пейджери, бездротові ком'ютерні мережі, стільникові мережі та ноутбуків. Стрімкий розвиток бездротових мереж був зумовлений прогресом у радіочастотній та мікрохвильовій техніці та переходом від аналогових до цифрових радіочастотних технологій. Успіхи технології МДН-транзисторів став ключовим компонентом для радіочастотних технологій, що є основою цифрових бездротових мереж.

Висновки та перспективи.

Зараз важко уявити собі теперішній світ без телекомунікацій, бо ми їх використовуємо майже в усіх аспектах нашого життя. Можливо в найближчому часі з’являться нові телекомунікацій і комунікацій взагалі.

Література:

1. *https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%97*
2. *https://amrita-cs.com/telecommunication_systems/telecommunication-and-active-network-equipment/*

TELECOMMUNICATIONS OF THE FUTURE STARLINK

Tuzhilin Denys
State University of Telecommunications
Educational and Scientific Institute of Information Technologies
Kyiv

In the process of development of society, people have a need for fast transmission of information over long distances. For this reason, the first telecommunication devices began to appear, allowing the transfer of information between two or more objects.
Nowadays, there are many communication systems that allow us to realize the dreams of our ancestors. But even among this multitude there are those units that not so long ago could only be vaguely imagined.

Not so long ago, a rising star in the digital industry, SpaceX, launched the Starlink project.

Starlink is a 2015 idea made by extraordinary genius, entrepreneur and computer engineer Elon Musk. Starlink is a network of satellites orbiting our planet. According to the company's idea, such a satellite system will revolutionize all areas of information technology, due to a number of superior parameters different from the networks we are used to. Reliability, high speed, accessibility to everyone and this is only a small part of all those parameters, which until recently could only dream of any Internet user.

The satellite system of access to information will surprise no one. A technology that can be accessed at certain times of the day when the satellite is visible to the client device. This access technology is used everywhere in GPS navigation, television, in some special telephones and for accessing the global Internet.

The Starlink Internet distribution project, in contrast to similar satellite systems, is devoid of disadvantages with coverage due to the large number of autonomous satellites built into a peer-to-peer network. In such a network, each unit, a satellite, will simultaneously perform the functions of a client, as a network participant, and a server, as managing client segments. In addition, this technology should expand communication channels and increase access speed.

The system will not connect directly from satellites to the device, unlike the satellite communications systems of Iridium, Globalstar, Thuraya and Inmarsat. Instead, it will be tied to user

terminals with a diameter of 61 cm, which will have phased array antennas and track satellites.

Starlink network architecture:

- Space segment
- Ground segment
- Network Management System -provides management of the satellite communication network, setting a single time in the network, allocating frequency slots on satellites for the operation of subscriber and gateway stations, coordinating the operation of gateway and subscriber stations, maintaining billing, collecting data on transmitted and received information, collecting data on the state of the system.
- Gateway stations -provide information transmission from the Internet via satellite to subscriber terminals.
- User Terminal - a terminal that is installed on a building and distributes a Wi-Fi network to one or more accounts.

In 2021, according to SpaceX's plan, Starlink broadband Internet access will become available worldwide, and access to the network is practically unrelated to the presence of ground infrastructure, unlike cell towers.

Cellular communication slowly ceases to be relevant, being replaced by communication via the Internet. It can be assumed that the prospect of any Internet network will be precisely the communication between clients using ground terminals receiving signals from the satellite system.

It is also worth noting one more important advantage of such a network - it does not require Internet cables. This means that there will no longer be a need to purchase 1-meter internet cables and lay them through walls and ceilings. Such a move will undoubtedly bring the world of information technology closer to a wireless environment.

Literature:

1. *https://www.starlink.com/*
2. *https://www.comnews.ru/content/209438/2020-10-07/2020-w41/enciklopediya-starlink#toc7*
3. *https://ru.wikipedia.org/wiki/Starlink*

BRAIN-COMPUTER INTERFACE. NEW WAY OF TELECOMMUNICATION

Tuzhilin Denys
State University of Telecommunications
Educational and Scientific Institute of Information Technologies
Kyiv

Laziness is the engine of progress. Probably everyone imagined how to quickly learn a large amount of information in a short period of time. Or imagined the ability to move objects with the power of thought.

Modern developments in the field of information technology are engaged in the invention of the most amazing gadgets. From the largest devices to the smallest, aimed at minimizing effort, simplifying human life.

Brain-computer interface (BCI, neural control interface (NCI), mind–machine interface (MMI), direct neural interface (DNI), or brain–machine interface (BMI)) is a system for exchanging data between the brain and an electronic device. Such a device makes it possible to decode the neural signals of the brain and transmit the received data to the computer system.

For the first time, the DARPA research agency drew attention to this data exchange technology. But full-fledged development of the brain-computer interface began in 1970 at the University of California. These were the first experiments aimed at studying the transfer of information from the brain to a computer device, which allowed to restore the functions of hearing, vision and motor skills.

There are two types of BCI:

1) Invasive – systems implanted in a specific area of the brain matrix.
2) Non-invasive – systems capable of picking up electrical signals from the brain from the surface of the skin.

At present, non-invasive systems are inferior in the accuracy of receiving human signals, but they do not pose any danger in operation and implementation, unlike invasive implants.

A brain-computer device records sequential incoming electrical signals from the brain using electrodes. After that, the device processes the received data using the input circuits of the amplifier and converts them into digital signals. Then the microcontroller carries out the signal analysis procedure and converts it into commands for the executive device.

BCI systems are applicable in many areas of human activity. Most brain-computer devices, according to the old idea, are aimed at restoring damaged functions of the human body. But this technology is able to find itself in other areas, such as: remote access to devices, training neural networks, communication through data transfer directly from the brain to the brain, as well as the possibility of improving the characteristics of the human body. And this is only a small part of the technologies of the future based on brain-computer devices.

Literature:

1. https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BA%D0%BE%D0%BC%D0%BF%D1 % 8C% D1% 8E% D1% 82% D0% B5% D1% 80%

D0% BD% D1% 8B% D0% B9_% D0% B8% D0% BD% D1% 82% D0% B5% D1% 80 % D1% 84% D0% B5% D0% B9% D1% 81

2. *https://core.ac.uk/download/pdf/53095431.pdf*
3. *https://www.osp.ru/os/1998/04/179534*

СУЧАСНІ ПРОБЛЕМИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

Харченко Олег Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Телекомунікаційні системи та мережі – це комплекс технічних телекомунікаційних засобів та конструкцій для переадресації, комутації, надсилання та / або прийому символів, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого типу через радіо, кабель, оптичні чи інші електромагнітні системи між кінцевим пристроєм.

Телекомунікаційні системи та мережі відіграють важливу роль у соціальній та економічній діяльності суспільства та пропонують швидку або інтерактивну (діалогову) передачу інформації. Розвиток телекомунікацій повинен бути швидшим, ніж загальний темп економічного розвитку, і матиме вирішальне значення в найближчому та віддаленому майбутньому. Повільний темп розвитку телекомунікаційних систем та мереж призводить до зниження конкурентоспроможності української економіки [2, с. 322].

Телекомунікації відіграють важливу роль у прискоренні економічного та соціального розвитку. Беручи до уваги технологічні потреби в одночасному та гармонійному розвитку телекомунікаційних мереж, а також можливість розширеного використання сучасних та перспективних засобів телекомунікацій в Україні, слід розглянути основні проблеми функціонування телекомунікаційних систем та мереж:

- нерозвиненість мультисервісних телекомунікаційних транспортних мереж, які повинні бути необхідними для задоволення потреб споживачів телекомунікаційних послуг;
- збільшення пропускної здатності та пропускної спроможності мереж доступу для транспортування телекомунікаційних мереж із використанням передових технологічних рішень, зокрема радіотехнологій;
- низький рівень створення телекомунікаційних мереж у сільській місцевості за допомогою ефективних технологій;
- проблема адаптації системи нумерації телекомунікаційних мереж до європейських стандартів;

- неспроможність розробити та оптимізувати всі елементи телекомунікаційної інфраструктури української Інтернет-системи (включаючи систему транзиту Інтернет-трафіку) для забезпечення розвитку Інтернету в Україні;

- недостатня технічна можливість вибору постачальників телекомунікаційних та інформаційних послуг у телекомунікаційних мережах;

- відсутність технічних навичок щодо розвитку розподіленої інформаційно-довідкової служби та аварійних служб, зокрема служб підтримки доступу до цих послуг для абонентів мобільного зв'язку;

- низька науково-технічна та нормативна база для розширення мережі національних операторів на базі телекомунікаційних транспортних мереж із багатьма послугами

- низька реалізація радіо технологій для мобільного (мобільного) зв'язку та використання систем радіо доступу для абонентів;

- необхідність створення національної системи супутникового зв'язку.

Таким чином ступінь комп'ютеризації країни та ступінь її участі у світовому інформаційному суспільстві визначається розвитком інформаційного спілкування. Інформаційні мережі, засновані на телекомунікаційних мережах, становлять основу інформаційного спілкування.

Є три етапи еволюційного розвитку телекомунікаційних мереж: аналоговий, цифровий та етап інтеграції телекомунікаційних комп'ютерів. Перший етап знаменує еру аналогової телефонії, в якій мідні кабелі були основним середовищем передачі [1, с. 144].

Багатоканальні системи передачі побудовані за принципом частотного розподілу телефонних каналів. Інформація розповсюджувалась за принципом комутації каналів за допомогою телекомунікацій та комп'ютерної інтеграції і відзначалася успіхами в галузі електроніки, а також комп'ютерних технологій.

Література:

1. Телекомунікаційні системи та мережі: навчальний посібник для студентів спеціальності «Автоматизація та комп'ютерно-інтегровані технології» / Укладачі: Микитишин А. Г., Митник М. М., Стухляк П. Д. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.

2. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи: навч. посіб. [для студентів ВНЗ спец. 7.05090302 «Телекомунікац. системи та мережі», спец. 1«Телекомунікації та радіотехніка»] / І. В. Горбатий, А. П. Бондарєв; М-во освіти і науки України, Нац. ун-т «Львів. політехніка» — Львів: Вид-во Львів. політехніки, 2016. — 336 с.

ОБЛАСТЬ ЗАСТОСУВАННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

Чередниченко Андрій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Бездротова сенсорна мережа (БСМ) — розподілена мережа, що самоорганізується та складається із безлічі сенсорів і виконуючих пристроїв, об'єднаних між собою за допомогою радіосигналу. Область покриття мережі може становити до декількох кілометрів за рахунок здатності ретрансляції повідомлень від одного елемента до іншого.

Сенсори можуть працювати не лише від батареї, яка може працювати до декількох років, а й використовуючи інші способи, такі як, сонячні батареї, перетворення в електроенергію механічні коливання та використання енергії радіохвиль. Це дає більше можливостей для використання БСМ та дає можливість сенсорам працювати довше ніж з використанням батареї.

Основні причини використання БСМ:

- Потреба збирати данні з великої території;
- Неможливість прокладання проводів або висока імовірність їх пошкодження при використанню.

БСМ використовується для постійного збору даних, тому їх часто використовують не тільки для подальшого аналізу, а також при потребах автоматичного контролю. Наприклад, коли обладнання нагрілося до відповідного значення, сенсор повідомить це і система автоматично зменшить навантаження або повідомить диспетчеру.

Основні область застосування БСМ:

- Моніторинг довкілля (виявлення змін природнього середовища);
- Моніторинг у військових цілях;
- Охоронні системи;
- Пожежні сигналізації;
- Моніторинг промислового обладнання (моніторинг параметрів обладнання);
- Моніторинг стану транспорту;
- Моніторинг сільськогосподарських земель (моніторинг стані землі та посівів);
- Медичні імплантати для моніторингу стану здоров'я (моніторинг показників тіла та його місцезнаходження);
- Управління енергозбереження (моніторинг місцезнаходження людини для автоматичного включення

приладів освітлення, вентиляції, зміни температури повітря, вологості).

Таке різноманіття досягається універсальністю сенсорів які можна використовувати. Найчастіше це сенсори температури, руху, тиску, освітленості, рівня шуму, рівня вібрації, вологість, місцезнаходження, вітру, вмісту газів, вмісту речовин у воді.

Література:
1. https://en.wikipedia.org/wiki/Wireless_sensor_network

TCP/IP ПРОТИ OSI: У ЧОМУ РІЗНИЦЯ МІЖ ДВОМА МОДЕЛЯМИ?

Шелепенко Катерина Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Кожен день ми користуємося комп'ютерами та іншими девайсами, для різних потреб, таких як: спілкування с друзями, рідними; навчання; оплата комунальних послуг або придбання необхідних речей. Тому дуже важливо правильно оброблювати дані і пересилати їх з однієї точки в іншу. Завдяки таким технологіям модель OSI та TCP/IP ми можемо бути впевнені, що наші дані будуть правильно оброблені та не будуть втрачені.

Модель OSI - це модель, яка характеризує як повинні взаємодіяти компоненти мережевої комутації один з одним та описує обов'язки кожного з них. В моделі OSI представлено 7 рівнів:

- 7 рівень (Прикладний рівень). Забезпечує взаємодію мережі і користувача.
- 6 рівень (Рівень представлення). Відповідає за перетворення протоколів, кодування/декодування даних.
- 5 рівень (Сеансовий рівень). Цей рівень керує взаємодією між додатками, відкриває можливості синхронізації задач, завершення сеансу та обміну інформації.
- 4 рівень (Транспортний рівень). Забезпечує передачу даних від джерела до хосту призначення через одну або декілька мереж.
- 3 рівень (Мережевий рівень). Оброблює маршрутизацію пакетів через логічну адресацію та функції комутації.
- 2 рівень (Канальний рівень). Отримані дані в бітах (одиниця виміру розміру пакету) на цьому рівні пакуються в кадри, перевіряються на цілісність та виправляються помилки, після вони відправляються на мережевий рівень.

- 1 рівень (Фізичний рівень). Відповідає за передачу та приймання необроблених та неструктурованих даних в фізичному середовищі. Одиницею навантаження є біт.

Модель TCP/IP дуже схожа за характером з моделлю OSI, однак має меншу кількість рівнів. В ній представлено 4 рівня:

- 4 рівень (Прикладний рівень). На цьому рівні працює багато мережевих додатків. Ці програми мають свої особисті протоколи обміну інформацією.
- 3 рівень (Транспортний рівень). Відповідає за надання на прикладному рівні служб зв'язку сеансів і датаграмм. Його основні протоколи це TCP та UDP.
- 2 рівень (Мережевий рівень). Відповідає за адресацію хостів, упакування та функцію маршрутизації. Його основний протокол IP.
- 1 рівень (Канальний рівень). Описує, яким чином передаються пакети через фізичний рівень, включаючи кодування.

При знанні розділення рівнів, ми можемо діагностувати, де знаходиться проблема, коли пропадає з'єднання. Принцип пошуку проблеми полягає у тому що ми точно знаємо на якому рівні що оброблюється, тому при виникненні помилки ми можемо зразу зрозуміти на якому рівні вона виникла.

Враховуючи значення двох моделей, модель OSI-концептуальна, вона в основному використовується для опису, обслуговування та розуміння окремих мережевих функцій. TCP/IP в першу чергу використовується для вирішення проблем особливого характеру. OSI являється загальною та незалежною моделлю, однак велика кількість протоколів та систем базуються на ній. В той же час модель TCP/IP основана на стандартних протоколах.

Література:

1. TCP/IP vs. OSI: What's the Difference Between the Two Models? [Електронний ресурс] – Режим доступу: https://community.fs.com/blog/tcpip-vs-osi-whats-the-difference-between-the-two-models.html

ТРЕНДОВІ СИСТЕМИ КЕРУВАННЯ ВМІСТОМ

Шитіков Микита Андрійович
Державний університет телекомунікацій,
Навчально-науковий інститут Телекомунікацій
м. Київ

Інформаційні технології не стоять на одному місці. Кілька десятиліть тому необхідно було знати мови написання і мати великі знання в області веб-програмування для створення веб-сайту, але зараз системи керування вмістом є хорошою альтернативою ручному методу створення сайтів.

Система керування вмістом (CMS) – це програмне забезпечення на базі скриптів, які дозволяють керувати вмістом ресурсу, змінювати його, переглядати і контролювати. Автоматизовані методи створення сайтів розділяють структуру сайту на «дизайн» і «контент». В залежності від функцій веб-сайту, обирається найбільш вдала система керування вмістом. На даний момент існує безліч платних та безкоштовних движків, за допомогою яких створюються сайти будь-якої складності. Найбільш популярними є:

1. WordPress. WordPress початково призначений для блогів. Але за допомогою спеціальних розширень на ньому можна створити сайт будь-якої складності. Згідно із статистикою, на WordPress створена більша частина веб-ресурсів в мережі Інтернет (з тих, що створюються на CMS). Дизайн, управління, налаштування інтуїтивно зрозумілі. WordPress має величезну кількість шаблонів, як платних, так і безкоштовних. Присутні фільтри для пошуку необхідного типу. WordPress має відкритий код, тому кожен, хто знає мову програмування може кастомізувати шаблон, плагіни та інші речі під себе.

2. Joomla!. Суть використання Joomla! схожа з WordPress. Вона є безкоштовною і багатофункціональною системою керування вмістом. Цей движок досить гнучкий та простий в керуванні. Joomla! більше підходить для створення Інтернет-магазинів, корпоративних сайтів, соціальних мереж та візиток ніж для блогів та форумів. Так само як і WordPress, Joomla! має відкритий код. Базовий функціонал Joomla! дуже обширний. Одразу "з коробки" можна створити майже будь-який сайт та є всі необхідні інструменти для SEO-оптимізації. Додаткові компоненти завантажуються з каталогу розширень Joomla! [1].

3. Drupal. Drupal є широкоспрямованою CMS і має відкритий код. Через високий поріг входження, новачку складно освоїтися у веб-розробці. Тому, зазвичай, на цю систему переходять спеціалісти, які прагнуть отримати більше можливостей. Навички програмування обов'язкові для роботи, якщо необхідно використовувати весь спектр можливостей цієї CMS. Можна легко вносити зміни до файлів ядра. Ця CMS підходить для побудови масштабних сайтів, таких як Інтернет-магазини, корпоративні сайти, соціальні мережі і т.д. Використовувати її для блогів чи сайтів-візиток немає сенсу, адже затрати на подачу контенту та налаштування не окупляться. Якщо завданням є розробити сайт з різним

варіантом подачі матеріалів (одночасно продаж, блог, портфоліо) то Drupal є вдалим інструментом.

4. OpenCart. Це продукт електронної комерції, що розповсюджується по безкоштовній ліцензії з відкритим кодом і призначений для створення Інтернет-магазинів. OpenCart має інтуїтивно-зрозумілу адміністративну панель та низький поріг входу. Оскільки OpenCart орієнтована саме на створення Інтернет-магазинів, то одразу після встановлення движка, шаблону та додавання товарів до каталогу, можна оформляти замовлення. Беззаперечною перевагою цієї системи над іншими є можливість з однієї адмін-панелі керувати кількома магазинами [2].

5. InstantCms. InstantCms – це система керування вмістом з відкритими кодом. В основному цей движок призначений для створення соціальних мереж. З її допомогою також можна створювати блоги, сайти візитки, інформаційні портали, форуми, сайти новин. Соціальна мережа, створена за допомогою InstantCms, має все необхідне та характерне для соціальних мереж. Користувач має свій власний профіль, системи підписок, можливість вести як індивідуальну, так і групову бесіду, стрічки новин тощо. Так само як і в інших CMS, розширення функціоналу відбувається через плагіни та теми, які можна купити або встановити безкоштовно [3].

6. 1С-Бітрікс. Система є однією з найпопулярніших серед комерційних CMS. Використовується для створення великих сайтів, на кшталт Інтернет-магазинів, сайтів новин, корпоративних сайтів. Є вбудований модуль для SEO-оптимізації, який автоматично працює над просуванням сайту. 1С-Бітрікс є однією з найзахищеніших платформ, як безкоштовних, так і платних.

7. NetCat. NetCat є універсальною системою з відкритим кодом. На її базі можливо створити сайти будь-якої складності: бібліотеки, інформаційні портали, Інтернет-магазини, корпоративні сайти, візитки тощо. Після встановлення NetCat користувач одразу отримує адаптивний сайт. Існує кілька версій NetCat, що мають різні функціональні можливості: Standard, Business, Corporate, E-commerce та Extra. Можна створювати скільки завгодно сайтів з однієї придбаної ліцензії і керувати ними з однієї адміністративної панелі, чого позбавлені багато CMS.

8. UMI.CMS. Має відкритий вихідний код. Є п'ять редакції: Lite, Corporate, Business, Shop та Commerce. Всі вони відрізняються за кількістю та функціоналом модулів. UMI.CMS властива мультисайтовість. Немає необхідності встановлювати

движок на інший хосинг для створення ще одного сайту. Система керування вмістом одразу є адаптивною під різні пристрої. UMI.CMS є SEO-оптимізованим движком і він має ЛЗУ, можливість введення ключів, автоматичне створення карти сайту та файлу robots.txt. [4].

Література:

1. 20 причин использовать Joomla для создания сайта [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://wedal.ru/joomla.html

2. Гаврилов С. Обзор CMS OpenCart [Електронний ресурс] / Сергей Гаврилов. – 2019. – Режим доступу до ресурсу: https://site-builders.ru/cms-opencart

3. Обзор возможностей InstantCMS, плюсы и минусы движка для сайтов от российских разработчиков [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://cms-rating.ru/obzor-instantcms/

4. UMI CMS - обзор преимуществ как платформы для интернет-магазина [Електронний ресурс] – Режим доступу до ресурсу: http://www.shop-script.su/korobochnye/umi-cms

ЕТАПИ СТВОРЕННЯ ВЕБ-САЙТІВ

Шитіков Микита Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

В роботі розглянуто етапи створення веб-сайтів. Як і будь-яке складне завдання, створення сайту повинно бути розділене на менші підзавдання. Структуризація допомагає обійти великі втрати часу, сил і грошей. Вона є гарантією створення якісного сайту. Кожний етап є копіткою роботою.

Пайплайн створення веб-сайту у кожного розробника має свої особливості. Але усі компанії, які працюють у цій сфері, так чи інакше дотримуються певного базового алгоритму.

Основні етапи створення веб-сайтів такі:

1. Дослідження. Дослідження складається з двох частин – бріф та технічне завдання. Бріфом являється документ, який допомагає розробникам визначити вартість майбутнього сайту. В ньому замовник описує всі плани та ідеї щодо сайту. Розробники, ознайомившись з цим документом, визначають скільки часу необхідно буде витратити на розробку, на скільки це буде трудомісткий проект та якою буде його вартість.

Технічне завдання – це документ, в якому йде мова про те, які засоби будуть використовуватися, що доведеться робити, де розміщуватиметься сайт (хостинг), опис призначення сайту, вимоги до CMS і т.д. Розмір цього документу та ступінь його деталізації залежить від кількості вимог замовника. ТЗ може редагуватися, доки не буде досягнуто згоди між обома сторонами – замовником та виконавцем. Після підписання всіх документів можна переходити до наступного етапу [2].

2. Створення прототипу (прототипування). На цьому етапі малюється приблизний вигляд сторінок сайту – де будуть розташовуватися елементи (контакти, логотип, текст і т.д.). Якщо клієнта задовольняє результат, то він переноситься в графічний редактор і в ньому виконується ескіз. Завданням прототипу є схематичне зображення сайту – відображення елементів за допомогою блоків, без справжніх малюнків, тексту, банерів і інших елементів. Під час схематичного представлення також треба ухвалювати логіку сайту (що буде відбуватися на сайті при певних діях) [1, 3].

3. Дизайн концепція. Головне завдання полягає в більш детальному опрацюванні сторінок. На цьому етапі вимальовують деталі, щоб клієнт бачив, як буде виглядати сайт. Відбувається ухвалення шрифтів, кольорів, розмірів, розташування елементів тощо. Дизайн концепцію виконують по мінімуму, але так, щоб замовнику було зрозуміло як виглядатиме результат [1, 2].

4. Фінальний макет. Це останній етап для дизайнера. На цьому етапі створюються усі сторінки сайту у фінальному вигляді. І їх передають верстальнику. Головне не пропускати етапи створення прототипу та дизайн концепції і не переходити одразу до фінального макету. Бо в результаті сайт може виглядати гарно, але буде важкий в користуванні та не оптимізований.

5. Верстка. Верстальник на основі файлів фінального макету створює HTML-сторінки. При цьому, намагаючись їх максимально адаптувати. Сайт роблять багатоплатформенним, таким, щоб коректно відображався у різних браузерах і підключають до системи керування змістом. Це все завантажується на сервер де можна подивитися на сайт. Однак поки що він позбавлений динаміки.

Якщо замовник бажає, щоб сайт коректно відображався на мобільних пристроях, то на цьому етапі також розробляється адаптивний варіант. Якщо сайт є простим, на кшталт лендінгу, то його можна не прив'язувати до CMS, а сайт просто верстають на HTML та CSS мовах [1, 2].

6. Програмування. Тут починається наповнення HTML-сторінок кодом, написаним на будь-якій мові програмування. І тепер у сайта з'являються функції магазину, адміністративної панелі, контактні форми, каталоги і т.д. Але якщо розробляється «легкий» сайт, то програмісти не беруть участь в проекті [1].

7. Наповнення сайту. На цьому етапі сайт безпосередньо наповнюється статтями, товарами, фотографіями і т.д. Тобто всім тим, що було задумано на першому етапі. Якщо всі

попередні етапи пройдено, значить сайт готовий до призначення доменної назви та завантаженню на хост. Хоча вибір домену і завантаження на хост може виконуватися на будь-якому етапі створення сайту [1].

8. SEO оптимізація та просування сайту. На даному етапі сайт повноцінно працює, але він не приносить дохід і про нього знає мало користувачів. Створення семантичного ядра є одним з найважливіших пунктів для просування сайту. Семантичним ядром є список пошукових запитів (слова, словосполучення, морфологічні форми) на які повинні відповідати статті та сторінки сайту. Вони ще називаються ключами. Тобто те, що характеризує вид діяльності сайту.

9. Тестування. Сайт обов'язково перевіряють на наявність багів, працездатність, прибирають все зайве і доповнюють якщо цього вимагає ситуація. Це останній етап з точки зору технічного виконання [1].

Створення сайту це трудомісткий процес. Від ретельного виконання кожного етапу залежить життєздатність сайту в цілому. На практиці цих пунктів може бути більше або менше в залежності від ситуації.

Література:

1. Основные этапы создания сайта [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://impulse-design.com.ua/etapy-razrabotki-sajta.html

2. Этапы создания сайта с нуля [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://my-master.net.ua/osnovnye-etapy-sozdaniya-sajta/

3. Этапы разработки и создания сайта [Електронний ресурс] – Режим доступу до ресурсу: https://www.divier.ru/uslugi/etapy_razrabotki_i_sozdaniya_sayta/

ІТ-ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ СУЧАСНОГО ВИКЛАДАЧА

Щеглова Олена Андріївна
Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

Всесвітня мережа Інтернету дає нам змогу забути про застарілі методи викладання. Тепер тисячі книг, довідників, статей, наукових робіт можна знайти в електронному вигляді, що значно спрощує роботу сучасного викладача та дає можливість студенту самостійно опрацювати інформацію.

TED – всесвітньовідома конференція, яка була заснована у 1984 році Річардом Сол Вурменом та Гаррі Марксом. Місія конференції полягає в поширенні унікальних ідей. Усі лекції, семінари, конференції є у вільному доступі на офіційному сайті www.ted.com.

Як на мене даний ресурс корисний не тільки учням-студентам, а й самим викладачам, оскільки світ не стоїть на місці і з'являється потреба в оновленні своїх знань.

Prometheus — проект масових відкритих онлайн-курсів, заснований у 2014 році. Головною метою проекту є безкоштовне надання онлайн-доступу до курсів університетського рівня всім бажаючим. Лекції здебільшого складаються з відео уроків, після яких можна самостійно перевірити розуміння вивченого матеріалу.

iTunes U – каталог безкоштовних навчальних матеріалів, який пропонує більш 1 млн. безкоштовних лекцій, відео, книг і інших ресурсів для занять по тисячам навчальних дисциплін. Додаток iTunes U дозволяє студентам користуватися усіма книгами всередині програми. Також студенти можуть отримувати push-повідомлення про нову інформації вибраного предмета.

Єдиним недоліком є те, що додаток доступний лише для користувачів продукції компанії Apple.

MOOC – масові відкриті онлайн курси. Все почалося у 2000-х роках коли відомі світові університети почали викладати у вільний доступ записані лекції. Онлайн навчання проводять викладачі з найвідоміших світових університетів. І кожен студент дистанційного курсу має можливість поспілкуватися з ведучим особисто. Студенти мають можливість не тільки слухати інформацію, а й ділитися знаннями один з одним та виступати в ролі перевіряючих. Після здачі робіт студенти відразу отримують оцінку своїх знань. При цьому, кожен одержувач онлайн освіти має можливість перездати іспит або переписати тест.

Також викладач може за допомогою спеціальних додатків упорядкувати власні матеріали та поширювати їх студентам.

Google Classroom – створений Google для навчальних закладів з метою спрощення створення, поширення і класифікації завдань безпаперовим шляхом. Викладач створює електронний клас, у який долучає учнів через спеціальне посилання. Пізніше може відстежувати прогрес кожного студента, а після оцінки його роботи, викладач може повернути її разом з коментарями. Також додаток дозволяє викладачам архівувати курси наприкінці семестру або року. Коли курс архівується, він видаляється з домашньої сторінки та розміщується в зоні архівних занять з метою допомоги викладачам організовувати свої заняття. Коли курс архівується, викладачі та студенти можуть переглядати його, але не можуть вносити жодних змін, до тих пір поки його не буде відновлено.

Edmodo – дає вчителям змогу ділитися вмістом, створювати тести, вікторини та опитування, керувати спілкуванням з учнями, колегами та батьками. Працювати з системою можна як з комп'ютера, так і з мобільних пристроїв. Щоб розпочати працювати з додатком вчителю достатньо лише зареєструватися ввівши своє ім'я, прізвище, адресу електронної пошти, а також придумати пароль. Від школярів та їхніх батьків додатково буде потрібно вказати реєстраційний код, який їм видає вчитель. Викладач має можливість створювати різні групи: по предмету, по класах, за інтересами. Або ж він просто може таким чином об'єднувати користувачів для реалізації різних навчальних проектів. У групі можна розміщувати і зберігати файли: малюнки, фотографії, відеоматеріали. Також вчителі можуть видавати учням домашні завдання і здійснювати їх перевірку, створювати вікторини та опитування. В інструментарії є календар для фіксації занять, заліків та інших подій.

ClassDojo – був заснований в 2011 році Семом Чодхарі, британським шкільним учителем з економічною освітою, і Лайамом Доном, розробником ігор. Створений для швидкого і простого оцінювання класних та домашніх робіт. Також відстежує рівень поведінки учня. Батьки, зареєстровані в системі, отримують доступ до шкільного календаря, повідомлень від адміністрації школи та від конкретних вчителів, тобто усю необхідну інформацію.

Література:

1. *https://www.ted.com*
2. *https://prometheus.org.ua/*
3. *https://www.onlinecoursereport.com/state-of-the-mooc-report/*
4. *https://apps.apple.com/ru/app/itunes-u/id49021789*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Албакова Мадіна Мусаївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м.Київ

ВІРТУАЛЬНА РЕАЛЬНІСТЬ

Віртуальна реальність (англ. Virtual reality, VR, штучна реальність) - створений технічними засобами світ, який передається людині через його відчуття: зір, слух, дотик і інші. Віртуальна реальність імітує як вплив, так і реакції на вплив. Для створення переконливого комплексу відчуттів реальності комп'ютерний синтез властивостей і реакцій віртуальної реальності проводиться в реальному часі.

Віртуальна реальність - тривимірне комп'ютерне середовище, що взаємодіє з людиною. Людина занурена в цю середу за допомогою різних пристроїв (шоломи, окуляри і т.д.), є частиною віртуального світу, управляє віртуальними об'єктами і предметами. Ключовим елементом створення віртуальної реальності є комп'ютерна симуляція, для забезпечення якої використовуються різні периферійні пристрої, гарнітури. Найпопулярнішими гарнітурами VR є шолом і окуляри VR, повністю занурюють користувача у віртуальний простір, виключаючи зовнішнє звукове та візуальне вплив. У більшості випадків екран фокусується на все периферійний зір людини, щоб відключитися від зовнішнього світу. Часто пристрої віртуальної реальності включають в себе датчики стеження за рухом очей, захоплення рухів і т.п. Для розробки моделей віртуальної реальності існує спеціальний формат файлів VRML, що розшифровується як мова моделювання віртуальної реальності.

Віртуальна реальність активно застосовується в різних сферах життя суспільства. Наймасовіше поширення віртуальна реальність отримала в сфері розваг: віртуальні ігрові автомати, 5D/7D кінотеатри і т.д. У відеоіграх також використовуються елементи VR, включаючи PlayStation VR, PlayStation Eye, Microsoft Kinect, гарнітури Oculus Rift і HTC Vive.

Крім розваг віртуальна реальність використовується в медицині, наприклад, в психології для аналізу сприйняття, емоцій, психічного стану пацієнта, лікування психічних розладів, фобій. В якості терапії VR застосовують для зменшення больових відчуттів шляхом відволікання уваги пацієнтів.

Також пристрої віртуальної реальності часто використовують в сфері освіти для навчання новим навичкам,

наприклад, проведення операцій майбутніх лікарів, навчання водінню транспортних засобів (автомобілів, мотоциклів, поїздів, вертольотів, літаків і т.д.), так звані віртуальні симулятори.

У військовій сфері також використовують віртуальну реальність для військової підготовки кандидатів, курсантів і т.д. Аналогічно і в космічній сфері - для підготовки астронавтів до польотів (регулярно практикує NASA). У сфері мистецтва останнім часом також використовують пристрої для створення віртуальної реальності в музеях, виставкових залах, мультимедійних виставок.

ТЕХНОЛОГІЯ NFC

Near field communication, NFC («комунікація ближнього поля», «ближня безконтактна зв'язок») - технологія бездротової передачі даних малого радіусу дії, яка дає можливість обміну даними між пристроями, що знаходяться на відстані близько 10 сантиметрів; анонсована в 2004.

Ця технологія - просте розширення стандарту безконтактних карт, яке об'єднує інтерфейс смарт-карти і зчитувача в єдиний пристрій. Пристрій NFC може підтримувати зв'язок і з існуючими смарт-картами, і з іншими пристроями NFC і, таким чином, - сумісно з існуючою інфраструктурою безконтактних карт, вже використовується в громадському транспорті і платіжних системах. NFC націлена перш за все на використання в цифрових мобільних пристроях.

Головні плюси технології NFC:

- швидкість установки зв'язку між об'єктами (процес займає частки секунди);
- малий розмір пристрою;
- обмін даними з іншими пристроями;
- низький рівень енергоспоживання.

Завдяки цим особливостям NFC-датчики можна інтегрувати в невеликі за розміром гаджети.

Обмін даними з іншими пристроями:

Модуль можна використовувати для обміну інформацією між двома пристроями, що підтримують функцію NFC. Він дозволяє і передавати, і приймати файли з іншого смартфона. Обмін здійснюється за допомогою програми Android Beam. Вона є у всіх пристроях Android у версії не нижче 4.0.

Стандарт зв'язку NFC дозволяє передавати такі види інформації:

- посилання на веб-сторінки;
- координати місця розташування і маршрут на карті;
- контакти;
- посилання на додатки з Google Play.

Смартфон замість карти:

Телефони, що підтримують функцію NFC, можна використовувати в якості банківських або смарт-карт. Мобільний пристрій завжди знаходиться під рукою, чого не можна сказати про гаманець. Смартфон з NFC здатний стати альтернативою:

- віртуального гаманця (оплата товарів і послуг);
- пропуску в клуб, басейн або інше закрите установа;
- проїзним квитком в метро;
- бонусної картки.

ТЕХНОЛОГІЯ 5G

5G - це наступне покоління мобільних мереж, яке надасть набагато більш високі швидкості передачі даних, істотно знизить властиві 4G затримки і реалізує розрізання мережі на шари для віртуалізації єдиної мережі з підтримкою широкого спектру нових послуг, реалізувати які сьогодні неможливо навіть в кращих мобільних мережах.

5G (від англ. Fifth generation - «п'яте покоління») - п'яте покоління мобільного зв'язку, що діє на основі стандартів телекомунікацій (5G / IMT-2020), наступних за існуючими стандартами 4G / IMT-Advanced. Телекоммунікаціонний стандарт зв'язку нового покоління.

- Пікова швидкість передачі даних - як мінімум 20 Гбіт / с низхідній лінії зв'язку (тобто від оператора до абонента) і 10 Гбіт / с висхідній лінії зв'язку на мобільну базову станцію. В цілому, це означає 20-кратне збільшення швидкості в порівнянні з 4G LTE.
- Щільність з'єднання 5G - не менше 1 мільйона підключених пристроїв на квадратний кілометр.
- Мобільність - 5G дозволить абоненту пересуватися зі швидкістю до 500 км / год (у 4G - 120 км / ч).
- Енергоефективність - «сплячий» режим базових станцій і скорочення радіусу дії сот в щільних мережах дозволять значно зменшити енергоспоживання.
- Збільшення спектральної ефективності складе по низхідній лінії 30 біт / с / Гц, на лінії вгору - 15 біт / с / Гц.
- Затримка в ідеальних умовах мережі 5G становить до 1 мс (в порівнянні з 20 мс для LTE).

Де буде застосовуватися 5G?

Відверто кажучи, для простого користувача цілком достатньо 4G - цей стандарт дозволяє дивитися потокові відео і грати в ресурсомісткі ігри без істотних незручностей. До того ж, було б дивно, якби технологія, названа революційною, була розроблена для застосування тільки в розважальній сфері (хоча

і її, звичайно, не залишили без уваги). Насправді все набагато серйозніше, і п'яте покоління мобільних мереж охоплює куди більш важливі сфери життя, ніж перегляд серіалів.

Людина з кожним роком споживає все більше даних. Існуючі смуги спектра стають перевантаженими, що призводить до збоїв в обслуговуванні, особливо коли безліч людей намагаються отримати доступ до послуг мережі одночасно. 5G набагато краще справляється з тисячами синхронно підключених пристроїв: від мобільних телефонів до датчиків обладнання, відеокамер і вуличних ліхтарів.

З іншого боку, витрати на перехід до інфраструктури 5G будуть величезними. Мінімальна оцінка вартості будівництва і підтримки мереж 5G в Росії оцінюється НИИР в 164 млрд рублів (в США передбачаються витрати понад 200 млрд доларів на рік протягом наступних 5-10 років, і майже всі з них будуть оплачені приватними інвесторами). А це означає, що такі витрати повинні бути виправдані дійсно революційними змінами у всіх сферах життя.

Революція девайсів

Завдяки 5G набагато більше пристроїв зможуть одночасно приєднуватися до стільникових вишок, що буде сприяти розвитку інтернету речей.

Виробники зможуть вбудовувати чіпи в будь-які елементи своїх машин, і інженери будуть знати, яка деталь потребує ремонту або заміні. Фермери зможуть вішати сенсори на худобу, щоб знати, коли тварини потребують лікування, або вставляти їх в грунт, щоб стежити за необхідністю поливу. Деякі вчені навіть розглядають ідею дистанційній хірургії за допомогою роботів. «Найважливіше - мати достатньо потужності, - говорить колишній топ-менеджер Motorola Марті Купер. - 5G буде відігравати важливу роль в управлінні заводами ».

Люди в будинках зможуть підключати холодильники і пральні машини до інтернету, щоб визначати, коли вони потребують обслуговування. Бігуни - підключати до нього кросівки, щоб аналізувати свою швидкість і пройдену відстань. Імплантати для діагностики серцево-судинних захворювань зможуть автоматично відправляти інформацію лікарям.

Деякі з цих технологій доступні вже на 4G, хоча зазвичай потрібно під'єднання пристроїв до WiFi або смартфонам. Поява 5G дозволить їм бути завжди підключеними до інтернету, при цьому не сповільнюючи передачу даних в мережі.

ЗБІЛЬШЕННЯ КАМЕР В СМАРТФОНІ

Смартфони вже давно вийшли за рамки звичайних «дзвонилок» і перетворилися в мобільне інтерактивний пристрій, можливості якого можна

сміливо прирівняти до кишенькового комп'ютера. З смартфонів ми не тільки робимо дзвінки і використовуємо їх як засіб для зв'язку, але і слухаємо музику, дивимося відео, вирішуємо поточні робочі завдання і, звичайно ж, робимо фото. Завдяки своїй універсальності, ці гаджети вишитовхнули з ринку такі пристрої, як MP3-плеєри та фотоапарати типу «мильниця», які сьогодні вже практично не знайти на прилавках магазинів. І нехай до професійної фототехніки камери смартфонів ще не доросли, але амбіції у них прямо-таки грандіозні.

Скільки камер потрібно смартфону?

В одній камері не можуть поєднуватися зум, режим портрета, макрозйомки і ширококутний об'єктив. Тому їх частіше дві, рідше - чотири. А скільки потрібно, щоб отримувати якісний фотознімок - залежить від завдань і поставлених перед технікою цілей. Розберемо це питання на пальцях.

Навіщо смартфону дві камери?

Моделі з 2 камерами потрібні для імітації «боке» (розмитого фону). Цей ефект досягається завдяки тому, що додаткова камера допомагає смартфону розпізнати, де знаходиться основна дія.

Смартфони з двома камерами

«Аналізуючи» відбувається, пристрій відокремлює головне від другорядного і розмиває бекграунд. До отримання зображень, які за якістю не поступаються картинкам, зробленим дзеркальним фотоапаратом.

Навіщо смартфону три камери?

На відміну від подвійних, потрійні модулі поєднують в собі 5 функцій, за які хочеться сказати: «Спасибі!» виробникам.

1. *Доопрацьований суперзум*

Оптичний зум наближає до об'єкту, що знімається трикратно або п'ятикратно. Цифрове зумовское збільшення веде відлік від десятикратного до стократного наближення.

2. *Вдосконалений телеоб'єктив*

Стискає (наближає) візуальну дистанцію між зображеними об'єктами в кадрі.

3. *Ширококутова камера зі збільшеним захопленням*

Поміщає в кадр в рази більше подій.

4. *Точний чорно-білий (монохромний) модуль*

Вловлює ледь помітні перепади світла, що відбивається на яскравості знімка і чіткості фото в сутінках і вночі.

5. *Деталізована макрозйомка*

Можна фотографувати дрібні об'єкти, фото не буде «мутним».

Смартфон з трьома камерами

Якщо хочете на знімку більше опрацьованих деталей на вибраному об'єкті, - мікрокамера в допомогу. Потрібна глибина і різкість в темряві, виручить монохромний модуль. Чи

намагаєтеся 30 осіб помістити на груповому фото – широкоугольна камера не підведе.

Загалом, ви зрозуміли: телефон з трьома камерами замінить фотоапарат і відеокамеру. Аби було бажання знімати.

Навіщо 4 і більше камер в телефоні?

Окей. З 3-ма камерами розібралися. Впадання в крайність з чотирма-п'ятьма модулями теж виправдані. Камера отримує ще більше фішок.

Смартфон з 4 камерами

Макрокрамеру, як у Honor 20. Вона детальнейшим чином відобразить пилок на квітках або лапки павука.

Об'єктив зі збільшеним оптичним зумом виручить, якщо зйомка відбувається далеко від жаданого об'єкта. Буде видно все, як на долоні.

Модулі з II (для поліпшення якості фото) Не наводьте в звичному сенсі, але вони «зчитують» відбувається, і роблять фото чіткішим, а відео, менш змазаним навіть в ультра слоу-мо.

Література:

1. *https://iot.ru/wiki/virtualnaya-realnost*
2. *https://www.kp.ru/guide/nfc-v-smartfone.html*
3. *https://blog.allo.ua/kamery-v-smartfonah_2019-09-25/*

4.https://www.moyo.ua/news/zachem_telefonu_neskolko_kamer_ili_pochemu_4_luchshe_chem_2.html

USE OF CAUSAL GRAPHS IN THE TASKS OF AUTOMATED TESTING OF INFOCOMMUNICATION SYSTEMS

Albul Oleksandr, Holovko Serhiy
National Aerospace University
"Kharkiv Aviation Institute"

Software testing of infocommunication systems is an integral part of software development processes. This is the most expensive stage of development. Software testing usually involves a series of planned actions aimed at finding defects in the system. All software products have many defects and testing can reduce their number, but there is an axiom of testing which states: "It is impossible to find all the defects" [1, p.27]. However, in some cases, a critical defect in the software product that was not detected during the testing phase can lead to catastrophic consequences. In such systems, testing comes to the fore and requires more detailed elaboration and use of a large number of techniques for creating test scenarios.

Creating test scenarios for testing software of communication systems based on causal graphs requires the quality assurance engineer to determine the input conditions, output conditions and constraints according to the project specifications.

Software testing of infocommunication systems based on cause-and-effect graphs is a technique of generating test scenarios,

which uses a simplified digital-logical scheme. This technique comes from hardware engineering; however, it is adapted to software engineering. This is a black box testing technique where the input conditions are systematically combined to create test cases.

To generate test scenarios, you must first determine the input and test conditions from the software specifications. This process is called test analysis. Test analysis is not a complicated process, and it can be done simply by reading the software specification document. Everything in the software specification document can be a test condition. In addition, some conditions can be derived from experience that is not recorded anywhere. Test conditions may contain a wide range of possible conditions and may not contain accurate information. However, when generating test cases, the exact data of the software testing must be known. Test cases are derived based on software testing methods. Different software testing methods can derive different test cases from the same test conditions.

Myers [1, p. 124-170] identifies six stages of creating test scenarios from the specification based on cause-and-effect graphs.

At the first stage, the system decomposes into logical subsystems. The reason for this distribution is that the application of causal graphs to the whole system will be cumbersome and difficult to manage. Then each logical subsystem is decomposed into functions, and if necessary, the functions are decomposed into sub-functions.

The second stage is to identify the causes and consequences. In the context of testing, the causes are the inputs and the consequences are the outputs of the elements. The reasons may be different input conditions and equivalence classes, and the consequences may be the initial conditions and transformation of the system. Both causes and effects are determined from the specified software specifications. Every keyword or phrase in the software specifications can be a cause. Causes may include hardware events, API calls, and return codes. Conversely, effects may include equivalence class output conditions, dialogs, and interaction messages.

Moreover, all the results generated by the program are taken into account as an effect. Once the causes and effects have been determined, each cause and effect should be assigned a unique number or name. In addition, it is important to note that the assignment of a unique number or name should be done in such a way that the causes and consequences can be different. Because both causes and effects are represented by the same node shape in a causal graph, the only way to distinguish between causes and effects is through their unique identifiers or names [2, p. 43-55].

After determining the causes and consequences, they are depicted as nodes of the causal graph.

Relationships between cause and effect nodes are determined by analyzing the semantic content of software specifications. In this process, middle nodes can be created to represent combinations of causes. In addition, the logic of the combination of causes determines the type of middle nodes. Middle nodes are usually logical elements "AND" or "OR". Other elements of Boolean logic can also be applied. The middle nodes can connect not only the nodes of the causes but other middle nodes.

The next step is to define the constraints for the nodes. Some reasons may not be true at the same time, only one node can be true in one period of time. Also, some nodes may mask or require other nodes. Thus, all these limitations must be defined in the cause-and-effect column. Five general constraints are defined for causal graphs. Four of them are related to causes, and one of them can only be applied to effects. Restrictions "E", "I", "O" and "R" can only be applied to nodes - causes. Restriction "E" means exclusion. This restriction states that at least one of the nodes can be true. Moreover, all nodes can be false if only the "E" constraint applies.

The use of test creation techniques using cause-and-effect graphs greatly increases the likelihood of finding critical defects at the testing stage. This technique also reduces the number of test scenarios.

One of the disadvantages of this technique is the difficulty of creating graph trees for large systems and the time spent. The problem of complexity is solved by the fact that the quality assurance enfineer grinds the software product to a functional level.

Using software to create a graph tree also significantly reduces the time to create test scenarios.

A promising way to improve based on the algorithms of the obtained test scenarios, it makes possible to create automation test-cases.

References:

1. Mayers, GJ The art of software testing (2nd edition). [Text] / GJ Mayers– M.: USA: John Wiley & Sons Inc., 2004 - 257 p.

2. Bender, R. Cause-Effect Graphing User Guide (1st ed.). [Text] / R. Bender - M.: USA: Bender RBT Inc., 2008 – 159 p.

ШТУЧНИЙ ІНТЕЛЕКТ У ВСТАНОВЛЕННІ НОВОЇ ЕРИ «РОЗУМНОГО МІСТА»

Андрійко Володимир Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У часи, продиктовані, як ніколи раніше, необхідністю переходу до більш стійкої технологічно-соціальної парадигми, щоб уникнути негативних наслідків ресурсомісткої та бездумно опортуністичної філософії життєздатності, яка не виглядає далеко в майбутньому, Штучний інтелект (ШІ) має потенціал надати транспортний засіб для трансформації. ШІ з його функціями та можливостями глибокого навчання може бути використаний як інструмент, який дає можливість машинам вирішувати проблеми, які можуть реформувати заміські ландшафти, як ми їх знаємо вже десятки років, і допомогти у встановленні нової ери - ери "розумного міста".

ШІ - це концепція, яка визначена як можливість системи правильно інтерпретувати зовнішні дані, вчитися на таких даних та використовувати це навчання для досягнення певних цілей та завдань за допомогою гнучкої адаптації [1]. Однією з ключових сфер, яку ШІ може визначити, є транспорт. Забезпечення мобільності та її вплив на розвиток міст можна значно покращити, використовуючи інтелектуальні транспортні системи загалом та, зокрема, автоматизований транспорт. Це новий різновид мобільності, який заснований на ШІ, незважаючи на свою машинну орієнтацію, повинен бути орієнтований на користувача, який "розуміє" та "задовольняє" його, ринки та суспільство в цілому. Потрібно вибудовувати довіру та усувати ризики, щоб цей перехід почав діяти. Пропонується новий концептуальний внесок, який детально обговорює мало вивчену взаємодію ШІ, транспорту та розумного міста, а також те, як це вплине на міське майбутнє.

Він конкретно охоплює ключові ініціативи щодо інтелектуальної мобільності, що стосуються підключених та автономних транспортних засобів (CAV), автономних персональних та безпілотних літальних апаратів (PAVs and UAVs) та Mobility-as-a-Service (MaaS), але також заходи, які можуть працювати як спроможні технології для транспорту, такі як як Інтернет речей (IoT) та Фізичний Інтернет (PI) або відображають більш широкі трансформації, такі як Industry 4.0.

Обіцянка автономного, пов'язаного, спільного та оцифрованого надання транспортних послуг є недостатньою, якщо це не полегшить зусилля, що ведуть до поліпшення збереження навколишнього середовища, ефективності використання ресурсів, підвищення продуктивності праці, соціальної інтеграції, охорони здоров'я та добробуту. Люди повинні вірити в те, що зміни можуть бути справді корисними для багатьох, що вони можуть стати активними та залученими учасниками нової міської екосистеми, і що вони можуть розумно використовувати можливості, надані зв'язком ШІ-транспорт-розумне місто.

В наш час ШІ змінив наше життя в багатьох аспектах, від напівавтономних автомобілів на дорозі до роботизованих

пилососів у наших будинках, і, можливо, буде продовжувати вторгнення в будь-яку сферу нашого життя, від охорони здоров'я до освіти, розваг та безпеки, в найближчому майбутньому [2]. Приклади методів ШІ, що прокладають собі шлях у транспортне поле, включають Штучні Нейромережі (Artificial Neural Networks (ANNs)), Генетичні Алгоритми (Genetic Algorithms (GA)), Імітація відпалу (Simulated Annealing (SA)), Штучну імунну систему (Artificial Immune System (AIS)), Оптимізатор колоній мурашок (the Ant Colony Optimiser (ACO)), Оптимізація бджолиних колоній (Bee Colony Optimisation (BCO)) та нечітка логічна модель Fuzzy Logic Model (FLM) [3]. Ці втручання AI мають потенційні додатки для транспортного засобу, інфраструктури, водія або користувача транспорту, зокрема, для того, як вони динамічно взаємодіють, забезпечуючи транспортну послугу, яка сприяє розширенню можливостей користувачів та підтримує взаємодію людина-машина.

Оскільки транспорт є найважливішим наріжним каменем для функціональності міста, розвитку та процвітання, революційний транспорт перетворює концепцію міста. Міська структура та розвиток транспортної системи тісно пов'язані, про що свідчать такі теорії, як теорія оренди міської землі та теорія розташування, які концептуальнізують зв'язок між транспортом та використанням міських земель [4]. Неможливо абстрагувати бачення міст завтрашнього дня від майбутньої конфігурації їх транспортних систем. Надання рішень для мобільності для боротьби із заторами, забрудненням та погіршенням навколишнього середовища за допомогою технології ШІ, яка здатна забезпечити кращі, швидші, чистіші та дешевші способи пересування, є основою, разом із застосуванням телекомунікацій та енергетики, того, що ми називаємо розумними містами і шлях вперед для міської науки.

Література:

1. Kaplan, A.; Haenlein, M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Bus. Horiz. 2019, 62, 15–25. [CrossRef].

2. Li, L.; Lin, Y.L.; Zheng, N.N.; Wang, F.Y.; Liu, Y.; Cao, D.; Wang, K.; Huang, W.L. Artificial intelligence test:

A case study of intelligent vehicles. Artif. Intell. Rev. 2018, 50, 441–465. [CrossRef].

3. Abduljabbar, R.; Dia, H.; Liyanage, S.; Bagloee, S.A. Applications of artificial intelligence in transport: An overview. Sustainability 2019, 11, 189. [CrossRef].

4. Knowles, R.D.; Ferbrache, F.; Nikitas, A. Transport's historical, contemporary and future role in shaping urban development: Re-evaluating transit oriented development. Cities 2020, 99, 102607. [CrossRef].

В МЕДИЧНІЙ ГАЛУЗІ

Артеменко Ярослав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Розвиток медицини в XXI столітті стикається з певними проблемами, серед яких варто виділити: зростаючий попит на управління хронічними захворюваннями та відповідне збільшення витрат на охорону здоров'я. Розвиток цифрової охорони здоров'я відбувався тільки у 2010-х роках, і таким чином вона все ще перебуває на етапі формування, як і ті виклики, що виникають разом з нею.

До основних напрямів інновацій у медицині, що охоплюються цифровими та інформаційними технологіями, відносять: телемедицину, електронні записи пацієнтів, електронні рецепти, електронні медичні бази даних, використання сенсорів/пристроїв для фіксації різноманітних показників пацієнта, використання мобільних додатків, збір та аналіз великих масивів медичних даних, використання штучного інтелекту в медицині.

В умовах сьогодення, варто використовувати цифрові рішення, які є доступними, адже вони можуть допомогти зробити лікарську практику більш ефективною, покращити при цьому якість життя у медицині та відкрити дорогу новим інноваціям у медицині [2].

Такими рішеннями, зокрема є медичні додатки для пацієнтів, що мають хронічні серцево-судинні захворювання, завдяки яким, пацієнт може краще розуміти та відслідковувати власний стан, фіксувати свої показники, а також, бути зацікавленими в підтриманні свого стану здоров'я на належному рівні в амбулаторних умовах.

Серед таких додатків варто виділити My BP Control та Angina Control. Завдяки технологіям штучного інтелекту та BigData є можливість обробляти значні об'єми даних і на їх основі робити відповідні висновки, в результаті чого, значно спрощується постановка діагнозів, а також вибору методів лікування.

Українськими компаніями, які займаються штучним інтелектом, а також BigData в інтересах охорони здоров'я є: VITech (відповідні роботи в напрямку Big Data та Data Science для проектів медичного напрямку), Waverley Software (здійснення певного програмного забезпечення для вбудовуваних систем різного призначення), Light IT (консалтинг в галузі Data Science для проектів різного напрямку, зокрема і для медицини), Lemberg Solutions (розробка стандартів безпеки для IT-проектів у сфері охорони здоров'я).

Важливість телемедицини полягає в тому, що відбувається спрощення контактів між лікарем та пацієнтом, а також, полегшення отримання медичних консультацій, завдяки використанню комп'ютерних та телекомунікаційних технологій, внаслідок чого менше витрачається часу при наданні медичної допомоги [1]. Впровадження телемедичних проектів в Україні здійснюють: Liki24, Yod.ua, MeViCS, Eliky, Vodafone Україна, Doc.ua, FORCE, Bookimed, Helsi та CancerLog.

Відсутність зворотного зв'язку для людей, що використовують протези є серйозною проблемою, внаслідок чого, вони не мають можливостей повністю покладатися на протез. Швейцарською компанією SensArs було розроблено інтерфейс для з'єднання протеза ніг із залишковими нервами, що знаходяться в стегні користувача, що дало змогу забезпечувати таким чином сенсорний зворотний зв'язок.

Модульна протезна кінцівка (Modular Prosthetic Limb) – протез руки, що була розроблена DARPA, в першу чергу для дослідницьких робіт, здійснює забезпечення зворотного зв'язку та багатовимірний контроль руки за рахунок електродів, що імплантовані у мозок.

Із 2017 року в Україні запрацювала система eHealth, завдяки якій забезпечується автоматизація обліку медичних послуг, а також здійснюється управління медичною інформацією в електронному вигляді. До системи eHealth на початку 2020 року було підключено 1 709 медичних закладів та 25 195 лікарів. Створення eHealth відбувалось спільними зусиллями міжнародних донорів, державних органів влади, організацій громадянського суспільства та громадських активістів [3].

Висновок. Розвиток медицини в майбутньому в значній мірі залежить від глибини її цифрової трансформації. Сучасні цифрові технології відкривають двері в медицину майбутнього: високотехнологічну, професійну та пацієнт-орієнтованою. Вони слугуватимуть новими ефективними каналами комунікації й помічниками для лікарів і пацієнтів. Звичайно, що технології не зможуть замінити висококваліфікованих лікарів ще довго, проте навіть зараз ІТ-рішення починають грати більшу роль в запобіганні хворобам і поліпшенні швидкості та ефективності реагування в критичних ситуаціях.

Література:

1. Нові цифрові рішення в охороні здоров'я. [Електронний ресурс] – Режим доступу: https://www.umj.com.ua/article/194134/novi-tsifrovi-rishennya-v-ohoroni-zdorov-ya.

2. Цифрові рішення в медицині – майбутнє чи вже реальність? [Електронний ресурс] – Режим доступу: http://lib.inmeds.com.ua:8080/ bitstream/lib/ 2149/1/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96%20%D1%80%D

1%96%D1%88%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%B2%20%D0%BC%D0%B5%D0%B4%D0%B8%D1%86%D0%B8%D0%BD%D1%96%20%20%D0%BC%D0%B0%D0%B9%D0%B1%D1%83%D1%82%D0%BD%D1%94.pdf.

3. Цифрові технології у медицині: майбутнє, що зовсім поруч. [Електронний ресурс] – Режим доступу: http://zdorovi.agency/blog/cifrovi-tehnologiyi-u-medicini-majbutnye-sho-zovsim-poruch/.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ВОКСЕЛЬНОЇ ГРАФІКИ В ГРАФІЧНИХ СИСТЕМАХ

Артеменко Ярослав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Ідея воксельної графіки базується на понятті тривимірного пікселя – кубічного одиничного об'єму з якого утворений моделюємий простір, при цьому вокселі можуть бути прозорими, залитими одним кольором або градієнтом кольору за кольорами вершин куба.

У комп'ютерній графіці вокселі використовуються як альтернатива полігонам. Під вокселем зазвичай розуміється віртуальний елемент, що відповідає набору з шести прямокутних полігонів. Воксельне моделювання може використовуватись у різноманітних областях людської діяльності, наприклад для отримання моделей, які мають відображати саме внутрішній стан об'єкту (томографи для отримання тривимірного зображення складних деталей та механізмів).

Розглядати воксельну графіку без спеціально розроблених алгоритмів оптимізації використання пам'яті, немає сенсу, тому що обсяг воксельного простору, який представляється вокселями настільки великий, що для невеликої сцени потрібні гігабайти пам'яті. Наприклад, при дискретності простору 1 сантиметр і розміру сцени 100 · 100 · 100 метрів, то кількість вертексів становить 10000 · 10000 · 10000 = 1012 штук, якщо в найпростішому випадку для одного вокселя потрібно зберігати тільки один колір, тобто 24 біта, то виходить, що така сцена займе 3 · 1012 байта або 273 гігабайти [1, с. 72].

Для сучасного використання моделі воксельної графіки розроблено безліч алгоритмів, які застосовуються для роботи з двомірної графікою. Основа цих алгоритмів стосується використання деревовидних структур, що дозволяють описувати стан не для одного конкретно вокселя, а для деякої їх сукупності. У найпростішому випадку воксель представляється утворенням з восьми вокселей меншого розміру, а ті в свою чергу, також розбиваються на вісім менших кубів і так далі. При такому підході, область простору має однакові характеристики

всіх вокселей з яких вона утворена і може бути описана одним великим вокселем, зменшуючи таким чином обсяг необхідної пам'яті для зберігання такого воксельного простору.

Нестиснені воксельні моделі (в порівнянні з векторними) вимагають набагато більший обсяг машинної пам'яті при обробці, тому поширення набули стиснені воксельні моделі, принцип яких заснований на використанні розрідженого воксельного октодерева. Порівняння властивостей полігональної та вексельної графіки представлено в таблиці.

Таблиця 1.

Порівняльна характеристика полігональної і воксельної графіки

	Полігональна графіка	Воксельна графіка
Опис	Метод представлення об'єктів у вигляді набору багатокутників	Метод подання до вигляді набору тривимірних об'єктів – вокселів
Переваги	Програмно і апаратно розвинена технологія. Використання ресурсів відеокарти. Відносно малі витрати пам'яті. Варіювання рівня деталізації	Подання внутрішньої структури. Для реалістичного відображення не потрібно допоміжних засобів. Великі можливості зміни об'єктів
Недоліки	Необхідність використовувати шейдери для реалістичного відображення дрібних деталей. Відсутня внутрішня структура. Складнощі з заломленням світла і подібними ефектами. статичність моделей	Значні вимоги до пам'яті. Більш низька якість зображення. Прив'язка точок до вузлів матриці. Однаковий рівень деталізації. Відсутність розвинених апаратних засобів

В сучасному програмуванні при 3D моделюванні об'єкти часто створюють в основному тільки двома способами: або за допомогою плоских полігонів – тим самим буде створена пустотіла модель без внутрішнього наповнення або за допомогою об'ємних кубиків – вокселей, які повністю заповнюють внутрішній простір 3D моделі, де кожен такий кубик несе в собі інформацію про те, чим він є, наприклад, шкірою, м'язами, кістками.

З огляду на те, що полігональні моделі пустотілі за своєю природою, то дуже важко моделювати їх поведінку в 3D просторі. Наприклад, якщо програмісту потрібно змоделювати

поведінку води в 3D грі, то він стикається з проблемою: як змоделювати хвилі на поверхні води або як змоделювати сплески води, адже вода в грі – це просто килим, утворений з трикутників блакитного кольору і під цією площиною нічого немає, а тим часом потрібно показати хлюпання води. Тобто треба показати відділення частин води однієї від одної у вигляді піни і сплесків і для цього доводиться вводити нові об'єкти в пам'ять комп'ютера, а управління цими додатковими об'єктами вимагає великого мистецтва саме від програміста, а не від дизайнера. Якщо ж воду моделювати через вокселі, то все стає набагато простіше, бо вся вода від поверхні океану і до дна складається з «атомів», які легко «відокремлюються» один від одного природним, з точки зору програміста, шляхом.

Для сьогоднішнього ринку програмування ігор вокселі не підходять, але вони є наступним етапом у розвитку комп'ютерної графіки. Однак, щоб піднятися на цей ступінь, комп'ютерам необхідно вирости над собою. Подібна історія вже мала місце, коли на екранах вперше з'явилися пікселі і настав кінець ері двомірної векторної графіки. Полігони ж існують в прямому родинному зв'язку з векторною графікою, а вокселі вкрай схожі з пікселями. Однією з новітніх перспективних технологій, що дозволяє робити ефективну деталізацію воксельних об'єктів є розріджене воксельне октодерево (sparse voxel octree). Його основними перевагами є: значна економія пам'яті, природна генерація рівнів деталізації (аналога mipmap-карт) і висока швидкість обробки в рейкастингу.

Література:

1. Меркулова, Е. В. Создание алгоритмов построения трехмерной воксельной модели на основании результатов СКТ [Текст] / Меркулова Е. В., Адамов В. Г. // Сборник научных трудов Sworld/гл. ред. Куприенко С. В. Иваново, 2015. Вып. 1, т. 2. С. 72–79.

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПО ДОГЛЯДУ ЗА ШКІРОЮ

Бабенко Марія Олексіївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В роботі розкривається тема "Роль сучасних інформаційних технологій" та розглядається поняття автоматизації процесів. Взагалі то, в сучасному світі автоматизація поширюється на усі сфери діяльності людства, але я знайшла доцільним розглянути сучасні засоби інформатизації на прикладі медичної галузі, а саме обрала дуже затребувану у наш час ланку медицини – косметологію. На сьогоднішній день одним з найбільш перспективних напрямків автоматизації медицини в цілому - є індивідуальні електронні медичні

консультанти-асистенти. Отже в результаті написання роботи, було сформовано та описано ідею мобільного додатку для аналізу стану шкіри людини.

У сьогоденні є значна кількість факторів, що зумовлюють пошкодження шкіри та мають накопичувальний ефект (екологія, харчування, сидячий стиль життя). Наразі кожному члену суспільства необхідно мати свого особистого мед-асистента для своєчасного аналізу своїх проблем та отримання цільових та індивідуальних порад щодо усунення проблем [1, с. 3-13; 2, с. 1,3-7].

Розробка даного додатку дає змогу користувачу отримати експрес-консультацію у будь-якій точці світу використовуючи лише свій смартфон. Асистент по догляду за шкірою просканує недоліки (зерна, клітини, рельєф) і дасть цінну пораду щодо усунення порушень здоров'я шкіри обличчя. Він надасть рекомендації щодо покращення стану шкіри. Ця програма забезпечує легкий доступ до особистих, інноваційних та надійних підказок про догляд за шкірою обличчя та навчає користувачів догляду та підтримки здоров'я свого обличчя. Додаток працюватиме за допомогою двох основних джерел інформації: сканування (для отримання особистої інформації користувача) та єдиної бази даних лікарів та інших користувачів для розвитку та порівняння даних. Ключову роль відіграватиме база даних знань лікарів-косметологів, на основі якої додаток буде спиратися у прийнятті рішень [3].

Які інші функції готовий запропонувати додаток:

✓ Відстеження та аналіз змін стану шкіри.

✓ Об'єктивна оцінка змін стану шкіри залежно від вашого способу життя та використовуваних продуктів.

✓ Точний аналіз дефектів шкіри (зерен, клітин, рельєфу, зерен) завдяки сучасним технологіям.

✓ Тест для визначення типу шкіри.

✓ Перевірка стану обличчя за допомогою сканування (надалі сппр обере необхідну стратегію лікування на основі бази даних та особистих даних користувача).

✓ Статті з практичними порадами щодо догляду за шкірою.

На основі роботи дерматологів та косметологів програма зможе сканувати та аналізувати отриману інформацію. Як саме відбуватиметься процес впровадження додатку у життя користувача:

1. Користувач має провести первинний аналіз стану своєї шкіри.

- Тест на тип шкіри: Людина проведе тест в програмі та з'ясує, який має тип шкіри. Це надасть змогу обрати найкращу програму по догляду за шкірою.
- Обстеження шкіри: Використовуючи комп'ютерні технології та штучний інтелект, додаток виявляє ваші прищі, клітини та прищі та визначає текстуру шкіри.

2. Відслідковування прогресу

- Щоденник шкіри: Щоб регулярно перевіряти недоліки шкіри та контролювати її стан, користувач має робити регулярні сканування та зберігати їх результати до щоденнику
- Моніторинг стану шкіри відбуватиметься щодня. Користувач скануватиме своє обличчя, а програма порівнюватиме збережені та нові дані і робитиме висновок щодо прогресу.
- Рекомендації щодо продуктів: На основі звіту про стан шкіри, програма пропонує перелік рекомендованих продуктів з урахуванням певного типу шкіри.

3. Лікування та підтримка

- Стрічка новин здоров'я. Користувач читатиме статті з практичними порадами щодо шкіри з різними дефектами та отримуватиме інформацію про останні тенденції у світі краси!

4. Результат. Користувач зможе поділитися своїми успіхами та досягненнями у соціальних мережах [4].

Література:

1. Фролов С.В., Куликов А.Ю., Остапенко О.А., Стригина Є.В. Медичні системи підтримки прийняття рішень. Науково-практичний електронний журнал Алея Науки №11(27). 2018р. С. 3-13. URL: https://alley-science.ru/domains_data/files/11December2018/MEDICINSKIE%20SISTEMY%20PODDERZhKI%20PRINYaTIYa%20REShENIY.pdf

2. Лисецький Ю.М. СППР для вибору елементного базису корпоративних інтегрованих інформаційних систем. Математичні машини і системи. Україна, Київ 2017р. № 3 ISSN 1028-9763. С. 1, 3-7. URL: https://core.ac.uk/download/pdf/132545857.pdf

3. Мимрина А.Л., Геллер Л.Н., Жилина Н.М. МедФармВістник Татарстану, 2012р. URL: https://mfvt.ru/informacionnye-texnologii-v-organizacii-okazaniya-farmacevticheskoj-pomoshhi-bolnym-otdeleniya-reanimacii-i-intensivnoj-terapii/

4. Халафян А.А. Аналіз та синтез медичних систем підтримки прийняття рішень на основі технологій статичного моделювання. Дисертація на здобуття наукового ступеня. 2010р. URL: https://pandia.org/text/77/372/26618.php

FEATURES OF JAVA, C ++ PROGRAMMING LANGUAGES AND THEIR DIFFERENCES

Babenko Yelizaveta Kostiantynivna
State University of Telecommunications
Educational and Scientific Institute of Information Technologies
Kyiv

The abstracts consider the concepts and main features of the two programming languages C ++ and JAVA. Their differences are given and revealed.

On the example of writing the program "Hello World!" a comparative analysis of writing in each of the programming languages. The rating of programming languages as of 2020 has been studied and the place that each of these languages occupies in this rating has been determined. Their significance for society as a whole is highlighted.

Nowadays, the era of information technology is developing rapidly. It is difficult to imagine your life without programming languages, which play an important role in everyone's daily life. For example, using any electronic device (smartphone, computer, etc.), we do not even think that the basis of their work is based on one of the programming languages. I believe that the main programming languages that are most popular for learning and use, without a doubt, include Java and C++.

JAVA is an "object-oriented distributed, multi-program multi-threaded multiprocessor interpretation, a reliable, secure, architecture-neutral, portable, high-performance, multi-threaded, and dynamic programming language." Java was developed in 1991 by a team of researchers led by James Gosling of Sun Microsystems and was once called Oak. Over time, Oracle acquired Sun Microsystems in 2010. Historically, it was planned that Java would be used in embedded chips for household electronic devices. Oak was renamed Java in 1995, just when it was redesigned to develop so-called web applications [1, p. 10-11]. This language is suitable for many purposes and in general, for example, is used in the development of: software for the banking system, video games (computer / phone «Minecraft»), mobile applications.

C++ is a "high-level programming language that supports several programming paradigms: object-oriented, generalized, and procedural, based on the C programming language.". The C++ language was developed Bjarne Stroustrup in 1979 under the name "C with classes". Later, in 1983, it was renamed to the more familiar name C++. In the 1990s, C++ became one of the popular general-purpose programming languages. Basically, it began to be used in the development of: software, video games(Warcraft), drivers, client programs and more. It is worth noting that this language had a significant impact on the further development of currently popular programming languages such as C# and JAVA.

In particular, the differences between them include many factors, despite the fact that Java has borrowed from C++ syntax. First of all, it should be noted that Java and C++ are object-oriented programming languages.

First, Java cannot support pointers, operator overloads, structures, templates, merges, conditional compilation and inclusion, and default settings. However, in turn, it can support so-called "links" and has something similar to the function of pointers in C++, but still pointers in Java can not perform arithmetic operations. In turn,

everything that does not support Java supports C++ (aggregation, templates, operator overloads, pointers, arithmetic pointers, conditional compilation, which is one of the main functions, default settings).

Second, Java does not have a "goto" or "const" transition operator, which does not provide multiple inheritance. In turn, in C++ has a transition operator, supports multiple inheritance (to eliminate ambiguity when using the keyword "virtual").

Third, Java can support automatic control of dynamic memory release, has built-in thread support (to create a new thread, and overrides the "run" method), has built-in support for comments on documentation, can be interpreted (regardless of the platform) , has an overload method. At the same time in C++ supports destructors (the function can be activated automatically at object destruction), there is no built-in support of flows (for these functions use non-standardized libraries of the third parties), does not support comments to the documentation, generates object code (it may not run on different platforms) and supports method overload (including operator overload).

Fourth, exception handling in Java differs significantly because there are no destructors. However, in C++ you can not include the command "try / catch" even if this function generates an exception [4].

For example, I compare the writing of the first program "Hello World!" in C++ and JAVA:

Table 1

A comparative example of writing a program in two languages

C++	JAVA

#include <iostream>
using namespace std;
int main ()
{
	class HelloWorld
	{
	public static void main (String[] args)
	{
	System.out.println(“Hello World!”);
	}

cout<< "Hello World!"; return 0; }	}

Comparing one program "Hello World!" written in two different languages, we see in each variant the features of writing and it is not surprising, however it is also possible to notice that they differ in number of characters: in C++ (75), and in JAVA (87).

In general, the ranking of programming languages for 2020 shows that:

- by use in work: Java occupies the leading 2nd place (15.4%), C++ on the 6th place (5.8%).
- by according to personal preferences of users: Java takes the 4th place (13.9%), C++ on the 7th place (5.0%).
- by learning languages: Java ranks 4th (7.9%), C++ in 10th place (3.6%).
- as an additional programming language: Java ranks 5th (6.9%), C++ in 7th place (4.9%).
- by popularity in use in their projects: Java on the 3rd place (11.4%), C++ on the 6th place (6.9%) [3].

Thus, comparing the two programming languages, we can conclude that Java is more popular than C++ and has more opportunities for its application in different fields. But, separately, based on my own experience, I can say that C++ is much easier to understand and write than Java because it is from this language that my study of programming began. Also, I want to add that even if today C++ has a lower rating, it will always be studied, and Java will remain in the lead due to the wider use of this language.

Reference:

1. *Liang Y.D. (2014), Introduction to Java Programming, Comprehensive Version, 10th Edition. Prentice Hall, 1345 p.*

2. *Wikipedia, the free encyclopedia. // [Electronic resource]. – Access mode: // https://uk.wikipedia.org/wiki/C%2B%2B.*

3. *DOU. // [Electronic resource]. – Access mode: // https://dou.ua/lenta/articles/language-rating-jan-2020/.*

4. *Hillel Computer school. // [Electronic resource]. – Access mode: //https://blog.ithillel.ua/ua/articles/riznytsia-mizh-movamy-prohramuvannia-c-i-java.*

ІНСТРУМЕНТАРІЙ ДЛЯ УПРАВЛІННЯ ІЗОЛЬОВАНИМИ

LINUX-КОНТЕЙНЕРАМИ

Безручко Михайло Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Розглядання інструменту, який автоматизує розгортання застосунку у середовищах, щопідтримують контейнеризацію а також дозволяє керувати контейнерами на рівні ізоляції окремих процесів.

Docker — інструментарій для управління ізольованими Linux-контейнерами. Docker доповнює інструментарій LXC більш високорівневим API, що дозволяє керувати контейнерами на рівні ізоляції окремих процесів. Зокрема, Docker дозволяє не переймаючись вмістом контейнера запускати довільні процеси в режимі ізоляції і потім переносити і клонувати сформовані для даних процесів контейнери на інші сервери, беручи на себе всю роботу зі створення, обслуговування і підтримки контейнерів.

Docker складається з двох процесів:

1. Демона Docker, який запускається на гостьовій машині (якщо це Лінукс), або всередині VirtualBox середовища boot2docker (якщо це Windows або OS X).

2. Клієнта, через який можна взаємодіяти з демоном.

- Образ Docker (англ. *Docker image*) - містить операційну систему, застосунок і всі його залежності. Образи в Docker складаються з шарів. Якщо нам треба образ з веб-сервером, то ми беремо за основу образ з дистрибутивом операційної системи, додаємо залежність - веб-сервер, і записуємо це як новий образ, який матиме два шари - один з ОС, наступний з веб-сервером. Образами можна обмінюватись через DockerHub.
- Контейнер Docker - це запущений образ. Контейнери Docker можна запускати, спиняти, переміщувати і видаляти. Також можна зробити docker commit контейнера, що створить образз поточного стану контейнера.

Зазвичай для уникнення неочікуваної поведінки застосунку використовувались віртуальні машини (VM). Основна проблема у тому, що VM - це додаткова ОС, що працює поверх хостової, а це додаткові гігабайти для проекту. Часто ваш сервер обслуговує декілька VM, кожна з яких займає достатньо місця. А відомо,що більшість хмарних платформ стягує плату за використання додаткового простору. Ще один суттєвий недолік віртуальної машини — повільне завантаження. Також, більшість мов програмування, фреймворків та усі операційні системи мають свої пакетні менеджери. Якщо ваш застосунок

використовує нативний пакетний менеджер, вам може бути складно створити порт для іншої системи. Docker передбачає єдиний формат образу (image) для поширення застосунків між різними операційними системами та хмарними сервісами. Ваш застосунок тепер суцільний, має всі необхідні залежності та готовий до запуску.

Література:
1. *https://uk.wikipedia.org/wiki/Docker*
2. *https://codeguida.com/post/1837*

HTTP/2 ЯК РОЗШИРЕНА ВЕРСІЯ HTTP

Безручко Михайло Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

HTTP/2 що базується на попередній версії HTTP 1.1, яка була стандартизована. На відміну від HTTP 1.1 , HTTP/2 є бінарним. Змінились способи розбиття даних на фрагменти і їх транспортування міжсервером і клієнтом.HTTP/2 сервер може надіслати дані, які ще не були запитані клієнтом, але знадобляться клієнту для конкретної побудови сторінок.

SPDY - протокол прикладного рівня для передачі веб-вмісту, розроблений корпорацією Google. Основним завданням SPDY є зниження часу завантаження веб-сторінок та їх елементів. Це досягається за рахунок розстановки пріоритетів і мультиплексування передачі декількох файлів таким чином, щоб було потрібно тільки одне з'єднання для кожного клієнта. За задумом розробників, цей протокол позиціонувався як заміна деяких частин протоколу HTTP - таких, як управління з'єднаннями і формати передачі даних. SPDY просувається для включення до складу майбутнього стандарту HTTP/2.0.

HTTP/2 багато в чому грунтується на SPDY. Нова версія HTTP була створена робоча група Hypertext Transfer Protocol working group. У травні 2015 року специфікація HTTP/2 була опублікована як RFC 7540. Протокол HTTP/2 сумісніз HTTP/1.1. Зміни, спрямовані на усунення вузьких місць і підвищення продуктивності, багато в чому продовжують лінію SPDY. Розглянемо коротко найбільш важливі з них.

У HTTP/1.1 для кожного запиту потрібно встановлювати окреме TCP-з'єднання. У HTTP/2 мультиплексування дозволяє браузеру виконувати безліч запитів в рамках одного TCP-з'єднання. Завдяки мультиплексуванню статичні елементи завантажуються паралельно, і завдяки цьому істотно поліпшується продуктивність.

Нововведення HTTP/2 - це пріоритизація. Кожному запиту можна призначитипріоритет. Метод, який є основним в HTTP/2, полягає в наступному: браузер просить сервер завантажувати певні елементи контенту в першу чергу.

Наприклад, браузер може попросити сервер спочатку завантажити CSS-файлиабо JavaScript, а вже потім - HTML або зображення. У HTTP/2 пріоритизація є не обов'язковим, а бажаним методом. Однак мультиплексування без неї працювати належним чином не буде. Швидкість завантаження може бути навіть нижче, ніж HTTP/1.1. Ресурси з більш низьким пріоритетом будуть займати смугу, що призведе зниження продуктивності.

Сучасна веб-сторінка складається з безлічі елементів: зображення, JS, CSS та інші. У запиті на завантаження кожного з цих елементів браузер передає HTTP-заголовок. Відправляючи запитані елементи, сервер також додає до них заголовок. Все це пов'язане із зайвою витратою ресурсів.

У HTTP/2 заголовки передаються в стислому вигляді. Завдяки цьому зменшується кількість інформації, якою обмінюються між собою сервер і браузер. Замість алгоритмів gzip/deflate використовується HPACK. Це знижуєуразливість до атак типу BREACH.

У HTTP/1.1 є обмеження на кількість відкритих з'єднань. Щоб обійти це обмеження, доводиться завантажувати статичні ресурси з декількох піддоменіводного домену. Такий прийом називається доменним шардіруванням; він часто використовується, наприклад, для сторінок з великою кількістю зображень. Це допомагає збільшити швидкість завантаження, але разом з тим і створює додаткові проблеми. З переходом HTTP/2 необхідність в доменному шардіруванні відпадає. Ви можете запросити стільки ресурсів, скільки вам потрібно. Більш того, у випадку з HTTP/2 шардірування не поліпшить продуктивність, а призведе швидше до протилежного ефекту, так як створить додаткові TCP-з'єднання і буде заважати приоритизации.

Література:

1. *https://uk.wikipedia.org/wiki/SPDY*
2. *https://uk.wikipedia.org/wiki/HTTP/2*
3. *https://habr.com/ru/company/selectel/blog/278167*

HDD ПРОТИ SSD - ЯКА ТЕХНОЛОГІЯ ЗБЕРІГАННЯ ДЛЯ ВАС?

Бєлоножко Олексій Сергійович

Твердотільні накопичувачі (SSD) набирали оберти протягом останнього десятиліття, досягнувши тієї стадії, коли важко уявити використання нового ПК, який, принаймні, не включає в себе якусь форму зберігання SSD. Жорсткі диски - це стара застава, яка існувала ще з першої моделі 5 МБ у 1950-х роках, розміри якої досягають 20 ТБ.

На щастя, це не все або нічого рішення. Деякі з нас можуть відчувати, що жорсткий диск мертвий, але це скоріше особиста думка, ніж загальна істина. При порівнянні HDD та SSD основна різниця зводиться до ціни та продуктивності. Навіть найкращі твердотільні накопичувачі все ще коштують до трьох грн за ГБ або більше, тоді як жорсткі диски стартують менше гривні за ГБ. Це в чотири рази перевищує ціну за той самий обсяг пам’яті, але під керуванням Windows на жорсткому диску весь ваш ПК відчуває себе млявим. Твердотільні накопичувачі набагато швидше завантажуються під Windows і запускають улюблені програми.

Завдяки зниженню цін багато готових виробників ПК повністю пропускають жорсткий диск. Надішліть ПК чи ноутбук SSD накопичувачем на 1 ТБ, і більшість користувачів матиме більше ніж достатньо місця для зберігання. Для настільних комп'ютерів ви можете легко додати вторинну пам'ять у вигляді просторого жорсткого диска, якщо це необхідно, тоді як багатьом ноутбукам доведеться дивитися на зовнішні пристрої зберігання даних. Є доступні високошвидкісні SSD накопичувачі USB, які все ще можуть перевершити внутрішній HDD, а новіші SSD накопичувачі NVMe забезпечують ще більший виграш у продуктивності.

Як може підтвердити кожен, хто має цифрову бібліотеку ігор, сучасні вимоги до зберігання ігор не мають меж, нові ігри, включаючи оновлення та доповнення, легко піднімаються, а в деяких випадках і перевищують позначку 200 ГБ.

Коли PlayStation 5, Xbox Series X та Xbox Series S вирішують питання швидкого зберігання SSD накопичувачів, зміна, ймовірно, призведе до чергового значного зростання розміру назв AAA. Ігри в наступному поколінні, ймовірно, порушать 150 Гб, а деякі вже мають.

Однак це не тільки веселощі та ігри. Розглянемо традиційне резервне копіювання та зберігання носіїв. Немає необхідності створювати резервні копії ПК на високопродуктивному сховищі SSD накопичувачів. Якщо вам потрібно відновити з резервної копії, звичайно, це може

заощадити вам кілька хвилин, але відновлення з резервної копії в першу чергу буде набагато болючішим. Враховуючи довговічність та надійність сучасних жорстких дисків, вони все ще є найкращим рішенням для резервного копіювання ваших цінних даних.

Час завантаження Windows - це одне, але ігри, як правило, поводяться по-різному. Читається багато послідовних даних, і, як правило, у фоновому режимі ви не використовуєте багато інших речей, які потрапляють у вашу пам'ять. Практична різниця для геймерів між SSD та HDD дисками не така вражаюча. Це, безсумнівно, не непомітно, але ми говоримо не про хвилини, а про секунди.

Результати можуть виглядати досить суворо, якщо ви розглядаєте найкращий ефект проти гіршого. Результати завантаження локацій у грі можуть різнитись в 2-3 рази між SSD та HDD дисками.

Очевидно, що якщо у вас є гроші і ви хочете високопродуктивне обладнання, SSD накопичувачі завжди будуть найкращим рішенням. Але якщо вас більше цікавить цінність, HDD диски виглядають досить привабливо.

Література:

1. https://www.pcgamer.com/hdd-vs-ssd/

ЩО ТАКЕ СТРІМІНГ?

Бєлоножко Олексій Сергійович
Державний Університет Телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Перші веб-сайти являли собою прості сторінки тексту з, можливо, зображенням або двома. Однак сьогодні кожен, хто має досить швидке підключення до Інтернету, може транслювати фільми високої чіткості або робити відеодзвінки через Інтернет. Це можливо завдяки технології, що називається потоковою передачею.

Потокове передавання - це безперервна передача аудіо- чи відеофайлів із сервера на клієнта. Якщо говорити простіше, потокове передавання - це те, що відбувається, коли споживачі дивляться телевізор або слухають підкасти на підключених до Інтернету пристроях. Під час потокового передавання мультимедійний файл, що відтворюється на клієнтському пристрої, зберігається віддалено та передається через Інтернет кілька секунд за раз.

Потокове передавання відбувається в режимі реального часу, і це ефективніше, ніж завантаження медіафайлів. Якщо відеофайл завантажено, копія всього файлу зберігається на

жорсткому диску пристрою, і відео не може відтворюватися, поки весь файл не закінчиться. Якщо воно передається потоково, браузер відтворює відео, фактично не копіюючи та не зберігаючи його. Відео завантажується потроху, замість того, щоб завантажуватись весь файл відразу, і інформація, яку завантажує браузер, не зберігається локально.

Подумайте про різницю між озером і потоком: обидва містять воду, і потік може містити рівно стільки води, скільки озеро; різниця полягає в тому, що з потоком вода не знаходиться одночасно на одному місці. Завантажений відеофайл більше схожий на озеро, оскільки він займає багато місця на жорсткому диску (і переміщення озера займає багато часу). Потокове відео більше нагадує потік або річку, оскільки дані відео постійно, швидко надходять у браузер користувача.

Як і інші дані, що надсилаються через Інтернет, аудіо- та відеодані розбиваються на пакети даних. Кожен пакет містить невеликий фрагмент файлу, а аудіо- чи відеопрогравач у браузері на клієнтському пристрої приймає потік пакетів даних і інтерпретує їх як відео чи аудіо.

Потокові медіаплеєри заздалегідь завантажують кілька секунд потоку, щоб відео або аудіо могли продовжувати відтворюватися, якщо з’єднання ненадовго перервано. Це відоме як буферизація. Буферизація забезпечує плавне та безперервне відтворення відео. Однак за повільних з'єднань або якщо мережа має велику затримку, відео може тривати багато часу для буферизації.

Потокове передавання зазнає тих самих видів затримок та погіршення продуктивності, що й інші види веб-вмісту. Оскільки потоковий вміст зберігається в іншому місці, розташування хостингу має велике значення, як у випадку з будь-яким типом вмісту, доступ до якого здійснюється через Інтернет. Якщо користувач у Нью-Йорку намагається вести трансляцію з сервера Netflix у Лос-Гатосі, для досягнення користувача відеовмісту доведеться перетнути 3000 миль, а відео доведеться витратити довгий час в буферизації або навіть не відтворити зовсім. З цієї причини Netflix та інші провайдери потокового телебачення широко використовують розподілені мережі доставки вмісту (CDN), які зберігають вміст у місцях по всьому світу, які є набагато ближчими до користувачів.

CDN мають величезний позитивний вплив на продуктивність потокової передачі. Cloudflare Stream Delivery використовує Cloudflare CDN для зберігання відеовмісту в усіх центрах обробки даних Cloudflare по всьому світу; результатом

є зменшена затримка за короткий час запуску відео та зменшена буферизація.

Література:
1. *https://www.cloudflare.com/learning/video/what-is-streaming/*

ПРОБЛЕМНО-ОРІЄНТОВАНІ ПРОГРАМНІ ЗАСОБИ

Біловіцький Данііл Іванович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Проблемно-орієнтованими ППП називаються програмні продукти, призначені для вирішення складних комплексів задач в конкретній функціональної області. З усього різноманіття проблемно-орієнтованих ППП виділимо групи, призначені для комплексної автоматизації функцій управління в промислової і непромислової сферах і ППП конкретних предметних областей.

Основу багатьох сучасних систем моделювання (як і САПР) складають пакети прикладних програм (ППП). Комплексні програмні системи можуть об'єднувати кілька ППП.

Пакети прикладних програм можуть бути:

• об'єктно-залежними, проблемно-орієнтованими на певну предметну область;

• об'єктно-незалежними, методоорієнтірованнимі (інваріантними), тобто можуть використовуватися при моделюванні і вирішенні завдань з різних предметних областей.

Застосування таких методоорієнтірованних ППП часто менш ефективно:

• в них не враховується специфіка завдань конкретної предметної області;

• потрібно досить висока математична підготовка користувача, так як при використанні об'єктно-незалежних ППП необхідна спеціальна попередня підготовка завдання відповідно до особливостей застосовуваного методу.

Що ж собою являє проблемно-орієнтований ППП в загальному випадку?

Проблемно-орієнтований ППП - це комплекс спеціально-організованих програмних засобів, орієнтованих на вирішення завдань в певній предметній області науки і техніки, що відрізняється наступними головними рисами:

1) наявність проблемно-орієнтованої мови програмування (ПОМ) з Непроцедурного формою завдання на рівні, близькому до природного професійного мови даної предметної області. ПОМ не вимагає від користувача спеціальних знань в області алгоритмічного програмування;

2) виконання функції організації і планування обчислювального процесу - організація правильної послідовності виконання програмних модулів, обмін даними між ними, введення-виведення і зберігання інформації, тобто наявність досить універсального монітора.

Пакети прикладних програм автоматизованого проектування

Програми цього класу призначені для підтримки роботи конструкторів і технологів, пов'язаних з розробкою креслень, схем, діаграм, графічним моделюванням і конструюванням, створенням бібліотеки стандартних елементів (темплетов) креслень і їх багатократним використанням, створенням демонстраційних ілюстрацій і мультфільмів. Відмінною особливістю цього класу програмних продуктів є високі вимоги до технічної частини системи обробки даних, наявність бібліотек вбудованих функцій, об'єктів, інтерфейсів з графічними системами і базами даних.

Економічна інформація використовується головним чином в сфері матеріального виробництва. Вона служить інструментом управління виробництвом і виконуваних функцій управління поділяється на: на прогнозну, планову, облікову та аналітичну. У фінансово-кредитних установах вона пов'язана з економічною роботою фінансових і банківських установ з обслуговування клієнтів. Економічна інформація включає аналіз, контроль і ревізію, розробку заходів щодо поліпшення фінансово-економічного стану господарюючих суб'єктів та ін. Вона включає як текстові, так і числові, як правило, табличні дані. На основі відомостей про процеси виробництва, матеріальних ресурсах, процесах управління виробництвом, фінансових процесах, які циркулюють в економічній системі, і способів їх обробки за допомогою НІТ сформована економічна інформатика.

Обробка економічної інформації передбачає виконання логічних і арифметичних операцій над вихідними даними. Логічна обробка включає операції сортування (підбір, впорядкування, об'єднання), вибірку даних з інформаційної бази і т.п. Арифметичні операції - алгебраїчне додавання, ділення, множення і т.д.

Архітектура ППП включає такі основні складові:

- монітор пакета (керуюча програма);
- бібліотека програмних модулів (база даних);
- процесор з вхідного мови;
- сервісні засоби пакета.

Монітор пакета - спеціальна програма, яка за формулюванням завдання на вхідному мовою автоматично організовує виклик модулів в потрібній послідовності, забезпечує обмін інформацією між ними і керує процесом вирішення завдань. Введення моделі на вхідній мові можна здійснювати в довільному порядку.

Аналізатор забезпечує трансляцію вихідного тексту завдання на вхідній мові пакету у внутрішній мову ЕОМ. Іншими словами здійснюється розшифровка конструкцій, сформульованих на вхідній мові пакету і витяг з них інформації для організації роботи всіх інших програм пакету.

Планувальник обчислювального процесу визначає правильну необхідну ланцюжок, послідовність обробки модулів для виконання відповідних інструкцій.

Завантажувач-виконавець послідовно завантажує та виконує всі програмні модулі з обчислювальної схемою планувальника.

Література:

1. *https://tovaroveded.ru/lektsii-tovarovedenie/29-problemno-orientirovannye-avtomatizirovannye-informatsionnye-tekhnologii-v-tovarovedenii*
2. *http://um.co.ua/8/8-5/8-51280.html*
3. *https://studbooks.net/2088948/informatika/klassifikatsiya_paketov_prikladnyh_programm*

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

Біловіцький Данііл Іванович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Найпершою технологією пошуку шкідливих програм є сигнатурний аналіз. Сигнатурний аналіз є методом виявлення вірусів, що полягає в перевірці наявності в ділянках коду сигнатур вірусів. Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використовується практично у всіх сучасних антивірусних програмах.

Шкідливе програмне забезпечення (ШПЗ) – це програмне забезпечення яке може бути у вигляді коду або скрипта, впливає на коректну роботу комп’ютера, та збирає конфіденційну інформацію, застосовується для реалізації загроз інформації, що зберігається в системі.

Проблема ШПЗ загострюється з кожним роком, проте останнім часом змінилися цілі їх розробки і застосування, що обумовлює деякі особливості сучасних ШПЗ, і, як наслідок, вимагає наявності в антивірусних програмних засобах відповідних механізмів боротьби з ними. Якщо в недавньому

минулому ШПЗ розроблялися вузьким колом фахівців, а цілі їх розробки були вельми туманні, то зараз переважна більшість ШПЗ розробляється з метою отримання фінансової вигоди.

Найбільш поширені класи сучасних ШПЗ наступні:

Програми з потенційно небезпечними наслідками можна умовно розділити на три класи:

1) програми-"віруси";

2) програми типу "програмний черв'як" або "троянський кінь" і фрагменти програм типу "логічний люк". Вони мають можливість перехоплення конфіденційної інформації або вилучення інформації із сегментів систем безпеки;

3) програмні закладки або руйнують програмні впливу (РПВ) - узагальнений клас програм, обов'язково реалізують хоча б одну з перерахованих вище функцій програми з потенційно небезпечними наслідками.

Шкідливі (Malware) програми класифікуються на:

1) віруси і черв'яки;

2) троянські програми;

3) підозрілі пакувальники;

4) шкідливі утиліти.

Для виявлення ШПЗ використовують антивірусні програми. Один з способів виявлення ШПЗ – сигнатурний пошук.

Сигнатурний аналіз - метод виявлення вірусів, що полягає в перевірці наявності у файлах сигнатур вірусів.

Сигнатурний аналіз є найбільш відомим методом виявлення вірусів і використається практично у всіх сучасних антивірусах. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі.

Антивірусна база - база даних, у якій зберігаються сигнатури вірусів. Через те, що сигнатурний аналіз припускає перевірку файлів на наявність сигнатур вірусів, антивірусна база має потребу в періодичному відновленні для підтримки актуальності антивірусу. Сам принцип роботи сигнатурного аналізу також визначає границі його функціональності - можливість виявляти лише вже відомі віруси - проти нових вірусів сигнатурний сканер неспроможний.

Для боротьби з невідомими ШПЗ використовується евристичний аналізатор. Евристичний аналізатор призначений для пошуку невідомих вірусів. При перевірці якої-небудь програми аналізатор емулірує її виконання й протоколює всі її «підозрілі» дії, наприклад, відкриття або запис у файл, перехоплення векторів переривань і т.д. На основі цього

протоколу приймається рішення про можливе зараження програми вірусом.

Недоліком цього методу є те, що дуже часто мають місце випадки помилкового спрацьовування, при чому доволі часто вони перевищують кількість вірних.

Іншим методом є емуляція виконання програмного коду. Даний спосіб використовується для виявлення поліморфних і шифрованих вірусів, коли використання пошуку по контрольних сумах сигнатур не застосовується або значно ускладнено через неможливість побудови надійних сигнатур. Метод полягає в імітації виконання аналізованого коду за допомогою емулятора - програмної моделі процесора і середовища виконання програм.

Література:

1. *https://www.anti-malware.ru/practice/methods/malware-analysis-tools-explained*
2. *http://www.swsys-web.ru/code-of-popular-malware-analysis.html*

БЛОКЧЕЙН В МЕДИЦИНІ

Білоус Максим Леонідович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В технології або в будь-якому секторі потрібно революція. З розвитком технологій в швидкому темпі, немає сумнівів, що ми спостерігаємо нові зміни час від часу. Індустрія охорони здоров'я також повинна отримати максимальну користь з цих змін і забезпечити себе найкращими послугами і пропонованим рішенням. Технологія, про яку ми говоримо, і яка революціонізує охорону здоров'я - це блокчейн.

Сфера охорони здоров'я давно потребує змін і сьогодні є безліч можливостей для технології blockchain, щоб вона очолила трансформацію. Але технологія вже існує 8 років і ви матимете рацію, якщо скажете, що вона нічого не змінила. Крім, хіба що, фінансової сфери.

Інтерес до самої технології blockchain став помітний в останній рік. У тому числі і в сфері охорони здоров'я. Доказом зрослої потреби технології blockchain може служити результат дослідження, проведеного в жовтні 2017 року командою "Black Book" [Healthcare Industry interest in Blockchain is heating up, Black Book Survey, Q3 2017]. У ньому було опитано 88 споживачів системи охорони здоров'я (серед них, представники страхових компаній, споживачі медичних послуг) та 276 постачальників медичних послуг (що відповідають за технологічний процес фахівців, менеджерів і IT-фахівців).

"Black Book" виявив, що 19% керівників медичними організаціями та 76% представників, які оплачують медичні послуги, розглядали або вже застосовували рішення на основі технології blockchain.

70% всіляких організацій, які оплачують медичні послуги, очікують інтеграцію blockchain в існуючі системи і 9% постачальників медичних послуг збираються використовувати нову технологію вже в 2018 році.

Таким чином, підвищена увага до технології розподілених реєстрів призвело до розуміння потенціалу застосування технології в системі охорони здоров'я.

Ці умови дали благодатний грунт для команд і організацій, що бажають інтегрувати технологію blockchain в уже існуючі проекти або розробити нові, що відповідають вимогам високих технологій і роботи з великим обсягом даних.

Найбільші і масштабні розробки ведуться по стандартам відкритого вихідного коду і варто розуміти, що замість "винаходу велосипеда", іноді ефективніше приєднатися до розробки існуючого проекту і адаптувати його під локальний ринок. Тим більше, що сама технологія blockchain є міжнародною і децентралізованої. У цьому сенсі, наше прагнення зробити свій російський продукт просто не актуальне. 99% проектів мають повністю відкритий код і часто готові фінансувати розробку сторонніми командами.

Мета моєї доповіді - показати які проекти вже існують на стику медицини і технології blockchain. Які з них працюють, а які знаходяться лише на стадії прототипу або ідеї. В які процеси варто вбудовувати цю популярну сьогодні технологію.

Сучасна система охорони здоров'я.

Нинішня система охорони здоров'я застаріла. Вона сильно залежить від взаємодії між пацієнтом і лікарем і працює на обмежених даних. Обмежений аспект охорони здоров'я призводить до посередньої системі охорони здоров'я, яка як і раніше не може скористатися даними. Крім того, поточний процес отримання медичної допомоги є довгим і виснажливим. Все це призводить до неефективного поводження з пацієнтом.

Ланцюжок поставок і підробка ліків.

Ланцюжок поставок також страждає від несприятливого впливу ланцюжка поставок. Ця залежність призводить до маніпулювання цінами, запізнілим постачання ліків і багато чому іншому.

Підробка ліків є ще однією великою проблемою, оскільки вона веде до величезних втрат для всієї галузі охорони здоров'я. Нинішні системи ланцюжка поставок не здатні стримувати

контрафактні ліки. Це призводить до величезних втрат в 200 мільйонів доларів для індустрії охорони здоров'я.

Блокчейн може повністю змінити систему охорони здоров'я. Це може допомогти галузі охорони здоров'я подолати труднощі, з якими вона стикається. Наприклад, це може допомогти поліпшити універсальний доступ, цілісність, безпеку, відстеження і сумісність. Медичні додатки блокчейн є ключем до поліпшення поточного стану охорони здоров'я.

Завдяки блокчейну, кілька систем охорони здоров'я (HIS) можуть об'єднуватися і обмінюватися даними один з одним завдяки розподіленій структурі, яку він може запропонувати. Отже, які проблеми може вирішити блокчейн? Давайте перерахуємо їх нижче.

Література:

1. *https://medium.com/@brdt.pro/blockchain-в-медицине-примеры-использования-технологии-29fae16c5050*
2. *https://101blockchains.com/ru/блокчейн-для-здравоохранения/*

WIREGUARD VPN

Біріна Олена Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі - ознайомити слухачів з новою технологією VPN - WireGuard.

Мета дослідження - донести інформацію по темі, розділивши її на 4 пункти:

1) Що таке VPN?
2) Wireguard – новий протокол VPN?
3) Переваги та недоліки WireGuard.
4) WireGuard vs OpenVPN.

Результати досліджень

1) VPN (англ. Virtual Private Network - віртуальна приватна мережа) - це безпечне, зашифроване підключення між двома мережами або між окремим користувачем і мережею. Мережі VPN дозволяють користуватися Інтернетом, зберігаючи конфіденційність. VPN працює поверх Інтернету. Це означає, що підключатися до неї можна з будь-якої точки. Принцип технології полягає у створенні поверх мережі захищеного з'єднання (його можна назвати тунелем між комп'ютером і сервером). При з'єднанні відбувається шифрування і захист даних, що відправляються.

2) WireGuard - VPN протокол з відкритим вихідним кодом, який використовує найсучаснішу криптографію. Він націлений на те, щоб бути швидким, більш простим, економним, функціональним, ніж IPsec та більш продуктивним, ніж OpenVPN. Призначений для використання в різних умовах і може бути розгорнутий на вбудованих інтерфейсах, повністю завантажених магістральних маршрутизаторах і суперкомп'ютерах. Спочатку випущений для ядра Linux, тепер він є кросплатформним (Windows, macOS, BSD, iOS, Android). WireGuard нескладний, але потужний інтерфейс, який покликаний, бути простим в налаштуванні і розгортанні, як і SSH. В даний час він інтенсивно розвивається, але вже може вважатися найбезпечнішим, простим у використанні і найпростішим рішенням VPN. Його основні функції включають в себе простий мережевий інтерфейс, маршрутизацію крипто-ключів, вбудований роумінг та підтримку контейнерів (рис. 1). Поєднання надзвичайно високошвидкісних криптографічних примітивів і того факту, що WireGuard знаходиться всередині ядра Linux, означає, що безпечна мережа може бути дуже високошвидкісною. Він універсальний, тому що підходить як для невеликих вбудованих пристроїв, таких як смартфони, так і для повністю завантажених магістральних маршрутизаторів.

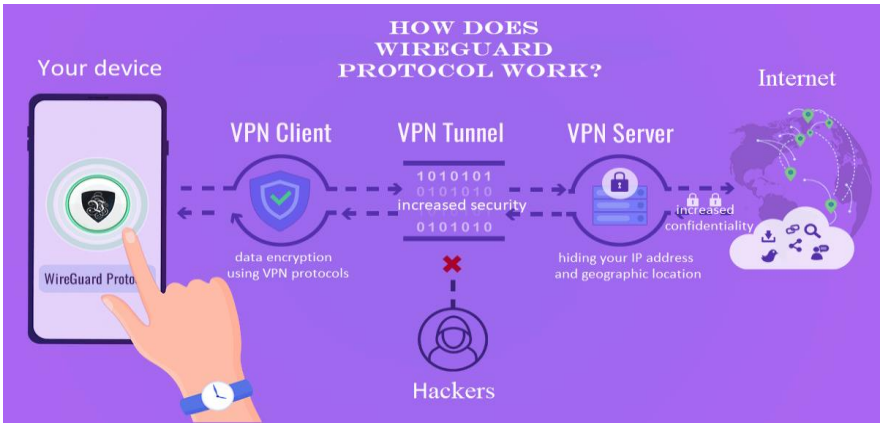


Рис. 1 – Як працює WireGuard

3) Переваги:

– відкритий вихідний код;

– компактна кодова база;

– простота перевірки;

– використовує сучасну криптографію: структура протоколу шуму, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF і т.п.;

– максимальна безпека;

– висока швидкість з'єднання;

– простий у використанні.

Недоліки:

– досі у розробці і доповнюється;

– може бути заблокований адміністраторами мережі.

4) Маючи близько 4000 рядків коду проти 70 000+ OpenVPN, WireGuard забезпечує кращий захист, в той час роблячи його більш гнучким та ефективним [4, с. 1].

OpenVPN є крипто-гнучким, тоді як WireGuard - ні. Шифрування для OpenVPN можна змінити або модифікувати відповідно до уподобань користувача. Для їх реалізації потрібні сертифікати безпеки. Отже, можна сказати, що OpenVPN - це протокол на основі сертифікатів. WireGuard використовує систему під назвою "Управління версіями". Він створює або випускає кращу чи вдосконалену версію свого продукту. Отже, оновлення WireGuard простіше. Відсутність криптоздатності робить його менш складним, а отже, більш безпечним. Це залишає меньше вразливих місць у WireGuard.

OpenVPN не виправдовує очікування коли справа йдеться про багатопотокові середовища. WireGuard інтегрований у простір ядра. Це дозволяє швидше використовувати багатопотокові можливості процесорів більш ефективно. Що стосується пропускної здатності та часу пінгу, WireGuard працює краще, ніж OpenVPN.

Компактна кодова база забезпечує просту перевірку на наявність вразливих місць у безпеці. Повний аудит WireGuard може бути виконаний однією людиною, в той час як аудит величезної кодової бази OpenVPN є складним завданням навіть для великої команди експертів.

Сьогодні багато організацій переходять на віддалену роботу, що призводить до збільшення попиту на VPN. Він не тільки допомагає безперешкодно переміщатися по всесвітній павутині, але також забезпечує необхідну безпеку для збереження даних. Це обов'язкова вимога для підприємств у всьому світі. На ринку є різні протоколи VPN, серед яких ми можемо обирати. OpenVPN до недавнього часу був на вершині списку. Однак WireGuard став новим фаворитом з моменту його запуску. Багато служб VPN прийняли WireGuard у свою інфраструктуру, оскільки вона стає більш популярною серед користувачів VPN у всьому світі. І завдяки покращеним швидкостям, надійності та вдосконаленому шифруванню, ми можемо очікувати, що популярність WireGuard продовжить зростати. Хоча попит на легкий і простий протокол в даний час низький, він, ймовірно, з часом зміниться. Саме такі рішення, як WireGuard, стануть наступним «галузевим стандартом» для VPN. Недоліки поступово виправляють, що в кінцевому

підсумку повинно зробити WireGuard більш привабливим для комерційних провайдерів VPN.

Література:

1. *https://www.vpnunlimitedapp.com/ru/help/vpn-protocols/wireguard-protocol*
2. *https://blog.avast.com/ru/chto-takoe-vpn-i-kak-eto-rabotaet-bazovoe-rukovodstvo-avast*
3. *https://te-st.ru/2018/05/22/what-means-vpn/*
4. *WireGuard: Next Generation Kernel Network Tunnel / Jason A. Donenfeld. - 2017. – С. 1. URL: https://www.wireguard.com/papers/wireguard.pdf*

ПЕРСПЕКТИВИ ШТУЧНОГО ІНТЕЛЕКТУ В ЦЕНТРАХ ОБРОБКИ ДАНИХ

Бойко Сергій Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м.Київ

Постановка задачі. Ознайомити слухачів з можливостями штучного інтелекту, їх вплив на центри обробки данних і користь яку вони несуть.

Мета дослідження. Поділити інформацію на наступні теми:

- зростання інтелектуального центру обробки даних;
- розумне використання енергії;
- інтелектуальна безпека;
- потенціал штучного інтелекту.

Результати дослідження. Центр обробки даних є серцевиною будь-якої IT-стратегії. Будь-який постачальник центрів обробки даних повинен переконатися, що він може підтримувати продуктивність та виправляти несправності, перш ніж це вплине на клієнта. Хоча це працювало в минулому, багато центрів обробки даних побудовано для більш простого, менш вимогливого віку. Як результат, деякі мовчки намагаються впоратися з вимогами швидкого прийняття штучного інтелекту, скорочено AI (Artificial Intelligence) [2]. Центри обробки даних все частіше використовують штучний інтелект для вдосконалення кожного аспекту своєї діяльності, від підвищення ефективності роботи мережі до підвищення надійності.

У багатьох центрах обробки даних досі зберігаються практики, які, здається, були минулими. Наприклад, центри обробки даних завжди були в стані підвищеної готовності щодо будь-яких несправностей в їхній інфраструктурі - від перегріваючого сервера до несправного блоку охолодження. Оскільки ніхто не може сказати, коли компонент вийде з ладу,

це вимагало від них постійних інженерів у самому центрі обробки даних або під час виклику.

Порівняйте це з набагато простішими машинами, такими як автомобілі або складальні лінії, які можуть мати тисячі датчиків, які постійно контролюють кожен компонент та роботу. Центри обробки даних можуть використовувати точно ту саму технологію для моніторингу своєї величезної, складної мережевої інфраструктури.

Центри обробки даних невидимі для пересічного користувача Інтернету, який не здогадується про величезну кількість споживаної ними енергії. Вони зобов'язані перед своїми клієнтами ефективно керувати споживанням енергії, щоб зменшити витрати. Тут штучний інтелект також повинен відігравати вирішальну роль. Навіть невеликі вдосконалення систем охолодження можуть мати значний вплив на енергоефективність.

Центри обробки даних є одними з найбільш безпечних місць на планеті, але вони не є невразливими. [1] Штучний інтелект - неоціненна зброя в боротьбі з кіберзлочинцями. З фізичної точки зору, вони можуть замінити пасивні камери на інтелектуальне відеоспостереження, яке відстежує людей по всьому приміщенню і може помітити підозрілу поведінку. З одного боку, штучний інтелект та машинне навчання мають вирішальне значення для виявлення нових шкідливих програм, які постійно розвиваються, щоб уникнути традиційних систем, які покладаються на розпізнавання підписів. Штучний інтелект може не тільки ідентифікувати підозрілий трафік, але також може запропонувати засоби для підвищення безпеки на периметрі або в самому центрі обробки даних.

Потенціал штучного інтелекту в центрі обробки даних майже безмежний, і ми змогли зосередитись лише на кількох сферах, де це принесе трансформаційні переваги. Прогностична аналітика може масово скоротити час, необхідний для виявлення та вирішення проблем інфраструктури, і навіть запобігти виникненню цих проблем. Штучний інтелект також дозволяє центрам обробки даних відповідати найскладнішим угодам про рівень обслуговування, знижувати експлуатаційні витрати, захищати час безвідмовної роботи і навіть покращувати відносини між установкою та її клієнтами за рахунок зменшення кількості інцидентів, що вимагають ескалації [3].

Література:

1. "Intelligent security" [Електронний ресурс] - https://www.datacenterdynamics.com

2. "Artificial Intelligence" [Електронний ресурс] - https://en.wikipedia.org/wiki/Artificial_intelligence

3. "Role of AI in Customer" [Електронний ресурс] - https://www.pointillist.com/blog/role-of-ai-in-customer-experience/

NEURALINK

Borys Oleksandr
State University of Telecommunications
Educational and Scientific Institute of Information Technologies
Kyiv

Human brain interface was an ambitious dream ever since computers became a part of our everyday life. Just imagine: you can complete tasks just by thinking about what you need to do! And that's only for starters. Two-way neural interface can become a cure for blind and/or deaf people by stimulating neurons to act just like if signal came from malfunctioning organ. Let's not forget entertainment value as well: watch movies without a TV and listen to music without having to wear the headphones! Possibility is limitless: entire Web can be at your disposal right inside your brain.

In June of 2016 Elon Musk, SEO of Tesla and SpaceX decided that the time has come and technology are sufficient enough to create a company, he called "Neuralink". Neuralink's main goal is to develop hardware and software to create neural interface, and they are doing great! There are working prototypes implanted on a lab rats, pigs, and even monkeys.

Implant itself is an application-specific integrated circuit (ASIC) with a grid up to 3072 very thin (4-6 μm) needle-like contacts implanted directly into subject's brain. Procedure must be so precise, Neuralink had to develop specialized robot-surgeon as a delivery method. Contact grid connected using gold wires to special connector that located on top of skin. There can be multiple implants to interact with each cortex. Using special ultra-high-band cables all of those connectors linked to computer running Neuralink's own software to receive, process, and respond on demand.

Neuralink plans to implant first human implant in 2021. As a subject was selected person with full-body paralysis. Four implants will be used: Primary motor cortex, Supplementary motor cortex, Premotor cortex, and in a Primary somatosensory cortex for providing a feedback. First task will be to achieve mind-controlled text input and a basic computer or smartphone navigation.

With development of technology Elon hopes to create wireless interface that can be connected to an ordinary smartphone to act as a host. In the future there is plans to create AppStore-like platform and open API for third-party developers so they can develop their own "applications".

Scientists community receives Neuralink interface with mixed reactions, main concern is that technology is not advanced enough to provide descent results as of now, however practically everyone

agrees that with enough time and money investment most of aimed tasks can be somewhat achieved.

References:
1. *https://en.wikipedia.org/wiki/Neuralink*
2. *https://ru.wikipedia.org/wiki/Neuralink*

DEEPFAKE DETECTION

Borys Oleksandr Anatoliyovych
State University of Telecommunications
Educational and Scientific Institute of Information Technologies
Kyiv

Artificial Neural Network (ANN) is a cutting-edge technology, that aims to solve problems that can't be solved using traditional algorithms. By enabling program to literally "learn" on similar examples, much like biological brains, developers can fine-tune each aspect of output result.

We've already saw examples of ANNs that can improve public health by detecting diseases much earlier that even most professional doctors, let alone classic software. Take, for example Google's ANN that predicts heart diseases by looking at patient's eyes [1]. But, in out IT world, where good comes, evil comes right away.

In early 2018 some developers adapted ANNs to swap one person's face in a video to another. Process woks by feeding a bunch of still images of one person's face and a video of another. Software matches face expressions, lips syncing, even head movements is not a big deal. Sometime later another developer created ANN that generates voice line of a person using nothing more, than a 10 seconds audio clip, and a desired text. Combination of both results is now called a Deepfake.

Software was leaked to the public, and, as a result, Internet flooded with a footage of famous people, faces of whom placed right into "adult" movies. Thankfully, this can't do much harm, mild annoyance of said famous people at the most, as well as a rush of managers to remove such footage. Despite the fact that a precedent is yet to be set, such Deepfakes can be a lot more harmful when used with politicians, businessman's, or any king of another public figure. From small misunderstandings, up to full scale wars – this all can be potentially achieved with Deepfake, when used in the right time, in the right place [2].

Fight fire… with fire! If we can create a Deepfake with an ANN, what the best way to detect it? You're right – another ANN. These exact thoughts came to the minds of IT giants, such as Microsoft, Amazon, Facebook. This companies created couple of challenges for public to solve, of course with a money prize, smallest

of which was a 1-million-dollar challenge [3]. The rules are simple: create an artificial neural network that will look at the video footage, plus audio clip, and using really tiny imperfections in input data will decide if given footage is legit or a crafted Deepfake. All of the challenges were completed successfully, and if necessity comes, IT giants will be on a full alert to save the world from political disaster.

References:

1. https://www.theverge.com/2018/2/19/17027902/google-verily-ai-algorithm-eye-scan-heart-disease-cardiovascular-risk

2. https://www.thenationalnews.com/opinion/comment/deepfake-technology-could-create-huge-potential-for-social-unrest-and-even-trigger-wars-1.755842

3. https://www.kaggle.com/c/deepfake-detection-challenge

ВИРІШЕННЯ ПРОБЛЕМИ ВІДХОДІВ В РОЗУМНОМУ МІСТІ

Бригинець Олександр Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Зростання обсягів відходів в значній мірі обумовлене двома чинниками: масштабною урбанізацією і зростанням промисловості. Сучасний спосіб життя по всьому світу виробляє набагато більше відходів на одного жителя, ніж всього десять років тому. За прогнозами ООН, до 2050 року 66% населення світу проживатиме в містах. Щоб витримати всі ці фактори, містах необхідний ефективний інструмент для управління відходами, моніторингу сміттєвих баків, а також оптимізації маршрутів збору.

Розумне місто є предметом обговорення протягом багатьох років, і багато міст в усьому світі все активніше застосовують стратегічні підходи переходу до розумного статусу.

Розумне місто представляє з себе цілісну концепцію розумної інтеграції інформаційних і комунікаційних технологій для моніторингу та управління міською інфраструктурою.

Мета таких заходів – поліпшити життя людей за допомогою підвищення рівня комфорту і безпеки, якості та ефективності обслуговування в різних сферах, оптимізації витрат на ряд високо експлуатованих ресурсів.

Розумний сміття – один з розділів концепцій Розумне місто і Розумний будинок, який передбачає оснащення процесів збору і переробки відходів різними датчиками для вирішення завдань оптимізації та ефективності, зокрема скорочення часу і енергії, необхідних для надання послуг з управління відходами. Серед компаній, що займаються розробкою таких систем можна виділити: EcubeLabs, IBM, Enevo, Compology, Bigbelly, OnePlusSystems.

Розумні сміттєві корзини сьогодні включають в себе безліч сенсорів, технологічних і функціональних можливостей. Їх кількість і вид визначається виключно виробниками і можуть включати в себе все що завгодно (деякі розумні сміттєві корзини можуть навіть самостійно пересуватися). Для зв'язку з іншими об'єктами розумного простору навколо, в більшості випадків використовуються бездротові мережі LPWAN або існуючі стільникові мережі.

Переваги технології Розумного збору сміття для Розумного міста:

- економія коштів і часу;
- легкість доступу до важкодоступних контейнерів;
- безпека;
- турбота про екологію;
- дистанційний контроль відходів.

Висновок

Сьогодні більшість муніципальних операцій зі збору відходів зосереджені на спорожнення контейнерів відповідно до заздалегідь встановленим графіком. Це абсолютно неефективно: спустошуються наполовину заповнені контейнери, неефективно використовуються міські активи і зайві витрати палива. Навпаки, переповнення сміттєвих баків призводить до зростання антисанітарії, і як наслідок шкідливого впливу на організми жителів.

Як приватні служби так і муніципалітети можуть скористатися технологією Розумного збору сміття. За невелику вартість сенсорної технології можна збільшити операційну ефективність і скоротити витрати в багатьох областях.

Хоч сектор технологій інтелектуального збору відходів все ще перебуває на ранній стадії, розумні сміттєві контейнери і датчики з підтримкою Інтернету речей (IoT) набувають популярності у всьому світі.

Література:

1. *https://www.ecubelabs.com/bin-level-sensors-5-reasons-why-every-city-should-track-their-waste-bins-remotely/.*
2. *https://www.postscapes.com/smart-trash/.*
3. *https://www.link-labs.com/blog/smart-waste-management.*

НЕЙРОННІ МЕРЕЖІ

Брик Олексій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій
м. Київ

Постановка задачі: ознайомити слухачів із суттю та використанням технології нейронних мереж.

Мета дослідження - донести інформацію по темі, розділивши її на 3 пункти:

1. Що таке нейронні мережі?
2. Навчання нейронних мереж.
3. Використання нейронних мереж.

Результати досліджень

1) Нейронна мережа (також штучна нейронна мережа, ШНС) - математична модель, а також її програмне або апаратне втілення, побудоване за принципом організації та функціонування біологічних нейронних мереж - мереж нервових клітин живого організму. Це поняття виникло при вивченні процесів, що протікають в мозку, і спробах змоделювати ці процеси. Першою такою спробою були нейронні мережі У. Маккалок і У. Питтса. Після розробки алгоритмів навчання одержувані моделі стали використовувати в практичних цілях: в задачах прогнозування, для розпізнавання образів, в задачах управління та ін.

ШНС являє собою систему з'єднаних і взаємодіючих між собою простих процесорів (штучних нейронів). Такі процесори зазвичай досить прості (особливо в порівнянні з процесорами, використовуваними в персональних комп'ютерах). Кожен процесор подібної мережі має справу тільки з сигналами, які він періодично отримує, і сигналами, які він періодично посилає іншим процесорам. І, тим не менше, будучи з'єднаними в досить велику мережу з керованим взаємодією, такі окремо прості процесори разом здатні виконувати досить складні завдання.

Нейронні мережі не програмуються в звичному сенсі цього слова, вони навчаються. Можливість навчання - одне з головних переваг нейронних мереж перед традиційними алгоритмами. Технічно навчання полягає в знаходженні коефіцієнтів зв'язків між нейронами. В процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними і вихідними, а також виконувати узагальнення. Це означає, що в разі успішного навчання мережа зможе повернути вірний результат на підставі даних, які були відсутні в навчальній вибірці, а також неповних і / або «зашумлених», частково спотворених даних.

2) Вибір даних для навчання мережі та їх обробка є найскладнішим етапом вирішення задачі. Набір даних для навчання повинен задовольняти декільком критеріям:

– Репрезентативність - дані повинні ілюструвати справжній стан речей в предметної області;

– Несуперечливість - суперечливі дані в навчальній вибірці приведуть до поганої якості навчання мережі.

Крім того, велику роль відіграє саме уявлення як вхідних, так і вихідних даних. Припустимо, мережа навчається розпізнаванню букв на зображеннях і має один числовий вихід - номер букви в алфавіті. У цьому випадку мережа отримає неправильне уявлення про те, що букви з номерами 1 і 2 більш схожі, ніж букви з номерами 1 і 3, що, загалом, не так. Для того, щоб уникнути такої ситуації, використовують топологію мережі з великим числом виходів, коли кожен вихід має свій сенс. Чим більше виходів в мережі, тим більшу відстань між класами і тим складніше їх сплутати.

В процесі навчання мережу в певному порядку переглядає навчальну вибірку. Порядок перегляду може бути послідовним, випадковим і т. Д. Деякі мережі, які навчаються без учителя (наприклад, мережі Хопфілда), переглядають вибірку тільки один раз. Інші (наприклад, мережі Кохонена), а також мережі, які навчаються з учителем, переглядають вибірку безліч разів, при цьому один повний прохід по вибірці називається епохою навчання. При навчанні з учителем набір вихідних даних ділять на дві частини - власне навчальну вибірку і тестові дані; принцип поділу може бути довільним. Навчальні дані подаються мережі для навчання, а перевірочні використовуються для розрахунку помилки мережі (перевірочні дані ніколи для навчання мережі не застосовуються). Таким чином, якщо на перевірочних даних помилка зменшується, то мережу дійсно виконує узагальнення. Якщо помилка на навчальних даних продовжує зменшуватися, а помилка на тестових даних збільшується, значить, мережа перестала виконувати узагальнення і просто «запам'ятовує» навчальні дані. Це явище називається перенавчанням мережі або оверфіттінгом. У таких випадках навчання зазвичай припиняють. У процесі навчання можуть проявитися інші проблеми, такі як параліч або потрапляння мережі в локальний мінімум поверхні помилок. Неможливо заздалегідь передбачити прояв тієї чи іншої проблеми, так само як і дати однозначні рекомендації щодо їх вирішення.

Все вище сказане відноситься тільки до ітераційним алгоритмам пошуку нейромережевих рішень. Для них дійсно можна нічого гарантувати і не можна повністю автоматизувати навчання нейронних мереж. Однак, поряд з ітераційним алгоритмами навчання, існують не ітераційні алгоритми, що володіють дуже високою стійкістю і дозволяють повністю автоматизувати процес навчання.

3) Нейронні мережі широко використовуються для прогнозування фінансового ринку. Для навченої мережі подається на вхід курс за сьогодні, вчора, позавчора і виходить відповідь на завтра. У цьому випадку мережа виведе залежність одного параметра від трьох попередніх. Якщо бажано враховувати ще якийсь параметр (наприклад, загальний індекс по галузі), то його треба додати як вхід (і включити в приклади), перенавчити мережу і отримати нові результати. Також нейронні мережі широко використовуються в хімічних та біохімічних дослідженнях. В даний час нейронні мережі є одним з найпоширеніших методів хемоінформатики для пошуку кількісних співвідношень структура-властивість, завдяки чому вони активно використовуються як для прогнозування фізико-хімічних властивостей і біологічної активності хімічних сполук, так і для спрямованого дизайну хімічних сполук і матеріалів з наперед заданими властивостями, в тому числі при розробці нових лікарських препаратів.

Література:

1. https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C#%D0%AD%D1%82%D0%B0%D0%BF%D1%8B_%D1%80%D0%B5%D1%88%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B7%D0%B0%D0%B4%D0%B0%D1%87

«РОЗУМНЕ» МІСТО

Брик Олексій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій
м. Київ

Постановка задачі - ознайомити слухачів із суттю та інтеграцією смарт-системи «Розумне місто».

Мета дослідження - донести інформацію по темі, розділивши її на 2 пункти:

1. Що таке «Розумне місто»?
2. Інтеграція «Розумне місто» в Україні.

З розвитком технологій наше життя стає все зручніше. Мобільні телефони, ноутбуки дозволяють нам отримувати, та обробляти інформацію не прив’язуючись до якогось робочого місця. Машини з вбудованими комп’ютерами спростили керування та пошук точки призначення. Розумний дім, який спрощує нам домашні клопоти. Логічно, що наступним виток розвитку технологій є «розумне місто», то що ж таки «розумне місто».

1) «Розумне місто» – концепція інтеграції декількох інформаційних і комунікаційних технологій і Інтернету речей для управління міським майном; активи міста включають, зокрема, місцеві відділи інформаційних систем, школи, бібліотеки, транспорт, лікарні, електростанції, системи водопостачання та управління відходами, правоохоронні органи та інші громадські служби. Метою створення «розумного міста» є поліпшення якості життя за допомогою технологій міської інформатики для підвищення ефективності обслуговування і задоволення потреб резидентів. Інформаційні і комунікаційні технології дозволяють міській владі безпосередньо взаємодіяти з спільнотами і міською інфраструктурою, та стежити за тим, що відбувається в місті, як місто розвивається, та якими способами дозволяють поліпшити якість життя. За рахунок використання датчиків, інтегрованих в режимі реального часу, накопичені дані від міських жителів і пристроїв обробляються і аналізуються. Зібрана інформація є ключем до вирішення проблем неефективності.

Виходячи з цього визначення «розумне місто» – це об'єднання технологій комунікацій та інформатизації для оптимізації життя людей в рамках одного міста.

2) В Україні реалізацію «розумного міста» вирішили почати з Києва. Даний проект включає в себе такі аспекти:

– Створення дата-центру;
– Створення системи камер;
– Ситуаційний центр;
– Будування опорної мережі для об'єднання всіх структурних підрозділів міста;
– Зони з відкритим Wi-Fi;
– Єдиний білет;

На даний момент реалізовано частково система камер, дата-центр, будова опорної мережі також триває, а її функції виконує орендована комерційна мережа. Єдиний білет проіснував недовго в тому вигляді якому він реалізовувався. Тепер замість початкової програми Kiev Smart City тепер її замінив «Київ Цифровий».

Отже, розумне місто безумовно буде використовуватись всюди і стане своєрідним символом цивілізації, яка мобільний зв'язок перед цим. В Україні інтеграція стикається зі своїми типовими труднощами такими як: брак коштів, корупція, відсутність кваліфікованих кадрів у владі які б розуміли процес інтеграції інформаційних та комунікаційних технологій.

Література:

1. *https://ru.wikipedia.org/wiki/%D0%A3%D0%BC%D0%BD%D1%8B%D0%B9_%D0%B3%D0%BE%D1%80%D0%BE%D0%B4*
2. *https://project.liga.net/projects/smart_city/*
3. *https://tech.liga.net/technology/article/kak-glavnoe-prilojenie-stolitsy-kyiv-smart-city-stalo-kiiv-tsifroviy-pochti-detektiv*

ПОКАЗНИКИ ЯКОСТІ ФУНКЦІОНУВАННЯ СЕНСОРНИХ МЕРЕЖ ЗВ'ЯЗКУ

Буц Олег Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Бездротові сенсорні мережі (БСС) є однією з основних компонент концепції Інтернету Речей і багато в чому визначають трафік для майбутніх мереж зв'язку. На сьогоднішній день БСС інтенсивно розвиваються завдяки відносно низькій вартості, швидкості розгортання та можливості застосування в умовах, коли важко використовувати кабельні мережі. Дані технології проникають в різні сфери життєдіяльності людини, такі як медицина, наука, фізичні системи безпеки, сільське господарство, робототехніка, промисловість, військова справа та багато іншого. Для визначення можливості реалізації тих чи інших послуг з на базі сенсорних мереж важливо знати їх параметри, технічні особливості та цілі використання, щоб забезпечити показники функціонування на належному рівні.

Як і інших мережах зв'язку, основна функція бездротоваої сенсорної мережаіполягає в передачі даних від точки А до точки Б тобто від користувача (або сервера) до користувача або до сервера. Мережа може передавати дані телеметрії або потокові дані, в залежності від послуги одержуваної користувачем. Велика частка послуг, для яких використовуються БСС, полягає в прийомі-передачі даних телеметрії і управління. Однак, при виборі відповідних технологій фізичного і канального рівнів можуть бути реалізовані і потокові послуги [1]. Потокові послуги припускають, що користувач передає або отримує регулярний потік пакетів, як правило, це послуги передачі звуку і відео.

Основні показники якості мережі можна розділити на три групи: доступність достовірність і тимчасові показники. До показників доступності відноситься ймовірність доступності послуги передачі даних, тобто наявність зв'язку між двома взаємодіючими вузлами. У БСС наявність зв'язності між двома вузлами залежить від різних чинників, наприклад, таких як: радіус зв'язку вузлів, спрямованості антен, від взаємного розташування вузлів мережі і характеризується ймовірністю зв'язності. Слід зазначити, що ймовірність зв'язності висловлює потенційну (фізичну) можливість доставки даних. Однак, наявність такої можливості є необхідним, але не достатньою

умовою для успішної доставки даних. Фактично можливість (ймовірність) доставки даних залежить від якості кожного з каналів на кожній з ділянок маршруту. Неможливість доставки може бути викликана перевантаженнями мережі трафіком [2], втратами пакетів в каналі, як через сторонних перешкод, так і з-за інтерференції між вузлами мережі.

Відсутність зв'язності в БСС призведе до часткового або повного порушення його працездатності. Для забезпечення і повного відновлення зв'язності спочатку, необхідно оцінити ймовірність зв'язності БСС. Потім шляхом додавання додаткових вузлів можна відновлювати зв'язність БСС.

Показник достовірності в свою чергу можна розділити на ймовірність втрати даних і вірогідність помилок в доставлених даних. Імовірність втрати даних або коефіцієнт втрат залежить від інтенсивності трафіку, кількості маршрутів довжини черг (обсяг буфера пам'яті) і т.д. імовірність помилок в доставлених даних залежить від різних чинників фізичної середовища.

До тимчасових показників слід віднести час доставки даних, варіацію затримки доставки даних (джиттер), пропускну здатність [3].

Отже, виконавши аналіз показав, для визначення можливості реалізації тих чи інших послуг з на базі сенсорних мереж важливо знати їх параметри, технічні особливості та цілі використання, щоб забезпечити показники функціонування на належному рівні.

Література:

1. Koucheryavy, Y. A. Wireless Technologies for IoT: M2M, 3GPP, EE and Cooperative / Y.Koucheryavy. - SPb: SUT, October 2017. – 141 p.

2. Кучерявый А.Е., Нуриллоев И.Н., Парамонов А.И., Прокопьев А.В. Обеспечение связности беспроводных сенсорных узлов гетерогенной сети. Информационные технологии и телекоммуникации. 2016. № 1 (9). С. 115-122.

3. Нуриллоев И.Н., Парамонов А.И. Эффективная связность беспроводной сенсорной сети. Электросвязь. 2018. №3. С.68-74.

ПРИКЛАД РЕАЛІЗАЦІЇ АРХІТЕКТУРИ СИСТЕМИ МОНІТОРИНГУ В РАМКАХ СИСТЕМИ INFRAMANAGER

Василенко Дмитро Валерійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Бурхливе зростання комп'ютерних мереж призводить до частих збоїв в їх працездатності. Тому необхідно покращувати існуючі способи контролю за функціонуванням локальних обчислювальних мереж.

Підтримка таких мереж вкрай важлива у зв'язку з тим, що вони є основною лінією передачі інформації між співробітниками на даний момент на

великій кількості підприємств. Недостатня пропускна здатність мережі, найбільш сильно проявляється в пікові моменти, викликає зниження продуктивності роботи співробітників, а також простої в роботі. Таким чином, для підтримки працездатності мережі необхідний ретельний моніторинг і діагностика її стану.

Для системи моніторингу, як для будь-якої складної систему стеження і управління, найбільш підходить трирівнева архітектура. Основними шарами в такій архітектурі є:

- Рівень даних (Data Level);
- Рівень логіки (Logic Level);
- Рівень призначеного для користувача інтерфейсу (User Interface Level).

На рис. 1. представлена схема взаємодії модулів (рівнів) системи моніторингу між собою і їх зв'язок з системою InfraManager.

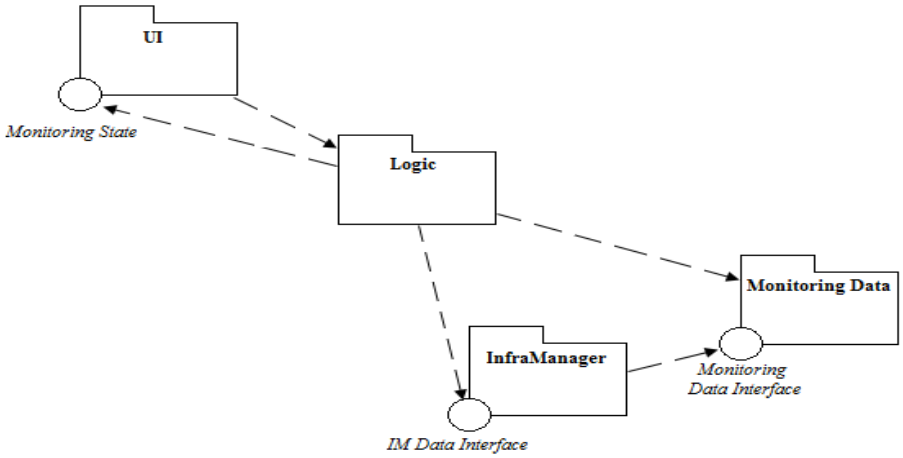


Рис.1. Архітектура системи моніторингу та її взаємодія з системою InfraManager

На першому рівні (Data Level) відбувається робота з даними. Якщо ви змінюєте джерело даних (SQL, Oracle, WMI) досить виправити функції цього рівня, щоб поміняти або додати нове джерело даних.

На даний момент є два джерела даних: база даних системи InfraManager і системна служба WMI.

На рівні логіки відбувається порівняння отриманих даних і прийняття рішення як цю інформацію інтерпретувати.

На рівні користувача інтерфейсу відбувається завдання параметрів моніторингу і виводиться звіт про поточний стан опитування.

Як видно зі схеми, система моніторингу пов'язується з InfraManager за допомогою інтерфейсу. Інтерфейс IM Data Interface дозволяє отримати доступ до зберігаються в системі даними для того, щоб їх порівняти з отриманими при моніторингу і при необхідності виправити. Також він

необхідний для ведення статистики моніторингу в системі InfraManager.

Інтерфейс Monitoring Data Interface дозволяє InfraManager отримати доступ до ще нових в базу даних пристроїв для додавання цієї інформації.

Література:

1. Кучерявый Е. А. Управление трафиком и качество обслуживания в сети Интернет. - СПб.: Наука и техника, 2016. - 336 с

2. Компьютерные сети и сетевые технологии: Пер. с англ./Марк Спортак, Френк Паппас и др. – К.: Издательство «ДиаСофт», 2015. – 726 с.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Верко Роман Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Сучасні інформаційні технології міцно увійшли в наше життя. Застосування ЕОМ стало буденною справою. Інформаційні технології відкрили нові можливості для роботи і відпочинку, дозволили багато в чому полегшити працю людини. Сьогодні я б хотів розповісти про деякі продукти інформаційних технологій які вразили мене.

1) MyBivy – додаток створений Тайлером Склужачі для розумних годинників який позбавляє людину нічних жахітть. Додаток Тайлер придумав для свого батька потерпілого від пост-травматичного синдрому після війни в Іраці. Принцип роботи додатку такий, що годинник розпізнає жахіття по частоті серцевих скорочень і за допомогою легких вібрацій, виводить людину з фази швидкого сна, але при цьому не будить власника годинника.

2) Osso VR - методика віртуального навчання молодих хірургів, яку використовують вже в 16 клініках Сполучених Штатів і Великобританії. Це - програма "симулятор хірурга", що дозволяє фахівцям тренуватися в проведенні операцій. Хірург працює з реалістичною моделлю пацієнта, на якій йому потрібно провести всі ті ж дії, які йому належить повторити в реальній операційній. Програма не тільки надає можливість потренуватися перед операцією, а й здатна оцінити рівень навичок лікаря - точність рухів, швидкість прийняття рішень, правильну послідовність процедур. Вона здатна визначити, чи готовий лікар до самостійного проведення операції, або слід ще попрацювати над навичками.

3) Rasberry Pi 400 – комп’ютер вбудований в клавіатуру. Зовнішньо комп’ютер виглядає як звичайна клавіатура, але в

середині замаскований спражній комп’ютер, який можна підключити до будь якого монітору. Купити його можна прямо зараз і ціна на такий гаджет починається від 70 доларів США.

Технічні характеристики:
Процесор - Cortex-A72 @ 1.8GHz
Об'єм ОЗУ – 4
Порти - Gigabit Ethernet, 2 × micro-HDMI, 2 USB 3.0 / 1 USB 2.0
Розмір – 286x122x23 мм

Література:
1)https://mediglobus.com/ru/how-is-virtual-reality-used-in-medicine/
2)https://evo.net.ua/raspberry-pi-400-personal-computer-unit/?gclid=EAIaIQobChMIjrXauMLr7gIViNOyCh3gaQDPEAYYASABEgInEvD_BwE
3)https://hightech.plus/2020/12/03/fda-odobrilo-pervoe-ustroistvo-dlya-borbi-s-nochnimi-koshmarami

АНАЛІЗ ПРИНЦИПУ ФУНКЦІОНУВАННЯ ТЕХНОЛОГІЇ IoT

Власенко Валерій Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Сьогодні ми стаємо свідками стійкого і постійного проникнення концепцій IoT у різні сфери промисловості, де з'являється можливість управляти засобами через хмарні мережі, які глибоко інтегровані з існуючими системами кешування і обчислювальної техніки. Підключені засоби (об'єкти) стають здатними отримувати важливі, своєчасні оновлення, з'являється можливість управляти даними від сенсорів/пристроїв.

Одним з перспективних напрямків розвитку концепції IoT є промисловий інтернет речей, який об'єднує машини, хмарні обчислення, аналітику і співробітників, щоб підвищити ефективність промислових процесів. Завдяки IoT промислові компанії можуть оцифровувати процеси, модифікувати бізнес-моделі, а також підвищувати продуктивність і ефективність, в той же час скорочуючи витрати.

На відміну від інтернету речей, в промисловому інтернеті порядок проведення обчислень і параметри обчислювальних операцій диктуються самою технологією (впорядкованістю) виробничого процесу. З'являється безліч альтернативних способів організації обчислювального процесу, що супроводжує і забезпечує необхідною інформацією виробництво.

Принцип роботи технології полягає в наступному: спочатку встановлюються датчики, виконавчі механізми, контролери та людино-машинні інтерфейси на ключові частини

обладнання, після чого здійснюється збір інформації, яка згодом дозволяє компанії придбати об'єктивні і точні дані про стан підприємства [2].

В типову IoT-систему входять:

- «Інтелектуальні» кінцеві пристрої (датчики, сенсори, контролери);

- Програмне забезпечення збору та обробки інформації, в т.ч. хмарні IoT-платформи, зі спеціалізованими інтерфейсами обміну даними (RESTful, Python API) і управління чергами повідомлень (AMQP, STOMP, MQTT);

- Провідні бездротові протоколи передачі даних на транспортному рівні моделі OSI - Serial, RS-485, MODBUS, EtherNet/IP, CAN bus, OPC UA, BLE, WiFi, тощо.

Оброблені дані доставляються в усі відділи підприємства, що допомагає налагодити взаємодію між співробітниками різних підрозділів і приймати обґрунтовані рішення.

Крім цього, компанії можуть замінити швидкозастаріваючий паперовий документообіг електронним, а також акумулювати експертні знання фахівців [1].

При обробці величезного масиву неструктурованих даних їх фільтрація і адекватна інтерпретація є пріоритетним завданням для підприємств. В даному контексті особливого значення набуває коректне подання інформації в зрозумілому користувачеві вигляді, для чого сьогодні на ринку представлені передові аналітичні платформи, призначені для збору, зберігання і аналізу даних про технологічні процеси і події в реальному часі.

Безперервний проактивний моніторинг ключових показників дає можливість визначити проблему та вжити необхідних заходів для її вирішення. Для зручності сучасні системи дозволяють візуалізувати умови протікання технологічних процесів і виявляти фактори, що на них впливають, за допомогою будь-якого веб-браузера. Оперативний аналіз допомагає користувачам швидше знаходити причини несправностей [1].

Завдяки таким рішенням виробничі дані перетворюються в корисну інформацію, яка необхідна для безпечного і раціонального управління підприємством.

Впровадження таких технологій дає можливість підприємствам з різних галузей економіки отримати певні переваги: збільшити ефективність використання виробничих активів на 10% за рахунок скорочення кількості незапланованих простоїв; знизити витрати на технічне обслуговування на 10%, удосконаливши процедури прогнозування і запобігання

катастрофічних відмов обладнання і виявляючи неефективні операції; підвищити продуктивність на 10%, збільшити рівень енергоефективності та скоротити експлуатаційні витрати на 10% за рахунок більш ефективного використання енергії.

Таким чином, нові технології дозволяють підприємствам різних галузей промисловості домогтися істотних конкурентних переваг.

Література:

1. Ли П.Архитектура интернета вещей / пер. с анг. М. А. Райтмана. – М.: ДМКПресс, 2019. – 454 с.: ил.

2.Hersent O., Boswarthick D., Elloumi O. The Internetof Things: Key Applications and Protocols, 2nd Edition. – Wiley, 2017, 370 p.

КОБОТ

Власюк Данил Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Коллаборативний робот (кобот) - це автоматичний пристрій, який може працювати спільно з людиною для створення або виробництва різних продуктів. Як і промислові роботи, коботи складаються з маніпулятора і змінювати програму пристрої управління, яке формує керуючі впливу, які визначають необхідні руху виконавчих органів маніпулятора. Коллаборативного роботи застосовуються на виробництві в рішенні задач, які не можна повністю автоматізіровать.

Коботи - напрямок у розвитку промислової робототехніки; "спільні роботи", які призначені для взаємодії з людьми і спільного використання робочого пространства.

У травні 1995 року Північно-Західний університет і корпорація General Motors оголосили про роботу над новим пристроєм - "інтелектуальним пристроєм-асистентом" (Intelligent Assist Device, IAD). Необхідність в таких пристроях була викликана тим, що на етапі кінцевого складання автомобілів було багато трудомістких процедур: установка панелей управління, дверей та ін. Зокрема, робочим на конвеєрі доводилося вручну встановлювати в автомобілі акумулятори масою по 18 кг. Автоматизувати ці процеси за допомогою існували на той момент технологій було неможливо, але IAD міг полегшити працю людей. Втім, він вирішував проблему зняття навантаження з робочих лише наполовину: дозволяв утримувати вантаж, управління здійснювалося за допомогою комп'ютера, але в рух цей пристрій наводилися за рахунок мускульної сили робочих. Першого кобота винайшли в 1999 році Едвард Колгейт (Edward Colgate) і Майкл Пешкін (Michael Peshkin), інженери

Північно-Західного університету. Заснована Колгейт компанія Cobotics до 2002 р випустила кілька моделей коботов. Але проривом в історії їх розвитку стали розробки датської компанії Universal Robots. Саме вона в 2008 році випустила коллаборативного робота в його сучасному вигляді: як автономний пристрій, здатне взаємодіяти з людиною.

У зв'язку зі стрімким "розмноженням" коботов виникає закономірне питання: чи замінять вони людей? Галузеві експерти не дають чіткої відповіді. З одного боку, деякі коботи беруть на себе роботу, перш виконувалася людьми. Наприклад, вже ведеться розробка коботов для пошиття одягу на звичайних швейних машинках. З іншого боку, коботи беруть на себе менш інтелектуальну та більш брудну, а іноді і небезпечну роботу. Крім того, для працівників-людей з'являються нові сфери зайнятості, такі як координація діяльності коботов і спостереження за виконанням поставлених перед ними завдань, перевірка і ремонт роботів. Це може вести не до скорочення, а до збільшення штату компанії, що використовує коботи. І поки ще залишається багато завдань (наприклад, вимагають дрібної моторики), з якими коботи впоратися не можуть. Але в міру вдосконалення технологій і усунення цих недоліків все більше компаній будуть впроваджувати коботов. "Вони дуже привабливі, щоб від них відмовитися, - каже Ден Кейра (Dan Kara), директор ABI з робототехніки, - сфера застосування цих роботів буде розширюватися" . Крім того, промисловий робот обходиться дешевше китайського робітника. При цьому він не хворіє, чи не вирощує дітей, які не страйкує і не потребує отпуске. Не дивно, що Міжнародна асоціація юристів (International Bar Association) пропонує ввести квоти на робочі місця для людей і ввести маркування товарів "зроблено людьми" (made by humans).

Література:

1. *https://www.cisco.com/c/ru_ru/about/press/press-releases/2015/10-07b.html*
2. *https://ru.wikipedia.org/wiki/Коллаборативный_робот*
3. *https://hightech.fm/2017/04/05/human_quotas*
4. *http://robotrends.ru/robopedia/katalog-kollaborativnyh-robotov*

ЩО ТАКЕ БЛОКЧЕЙН?

Власюк Данил Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Блокчейн - це нова концепція, яка кардинально змінює порядок передачі, обробки та захисту даних споживачів і організацій. Це настільки ж революційна технологія, як і мережа Інтернет, завдяки якій ми перейшли від звичайної пошти до електронної. Протягом найближчих десятиліть блокчейн змінить підхід до управління логістичними ланцюжками, проведенню комерційних операцій і обміну фінансовими активами. Блокчейн - це свого роду цифрова бухгалтерська книга, яка з плином часу постійно поповнюється новими записами. Ця «книга» децентралізована і захищена за допомогою засобів шифрування. Дані передаються по великомасштабної розподіленої комп'ютерної мережі, не схильною до людського фактору, і з даними резервування можна взаємодіяти в режимі реального часу без посередників. Мережа блокчейн не використовує традиційні IT-інфраструктури - закриті і відрізняються низькою керованістю. Блокчейн - це нова незалежна, прозора і захищена платформа безпечного зберігання, передачі і обробки конфіденційних і цінних даних. В даний час блокчейн найчастіше використовується для операцій з криптовалюта. Однак в перспективі технологія блокчейна має безліч варіантів застосування і може надати величезний вплив на найрізноманітніші сфери діяльності.

Використання блокчейна в сферах, не пов'язаних з криптовалюта Технологія блокчейна може знайти застосування практично у всіх галузях, в тому числі наступних:

- медицина і охорона здоров'я;
- фінанси і банківське обслуговування;
- страхування;
- інтернет речей (IoT) і мережі;
- цифрова реклама;
- кібербезпека;
- управління логістичними ланцюжками;
- прогнозування;
- хмарні обчислення;
- урядові установи;
- підприємства роздрібної торгівлі;
- ринок нерухомого майна;
- видавнича справа;
- некомерційні організації;
- енергетика;

Завдяки універсальності блокчейна ми вступаємо в епоху ефективного доступу до даних і безпечних транзакцій. Відпадає необхідність в посередниках, існування яких в рамках

традиційних моделей транзакцій неминуче призводить до появи вразливостей і залежностей.

Дуже часто значні зусилля витрачаються на ведення непотрібної звітності та зовнішні перевірки. Системи ведення обліку можуть піддаватися ризику шахрайства і кібератак. Обмежена прозорість може затягувати перевірки даних. Поширення IoT призвело до вибухового зростання обсягів транзакцій. Все це в сукупності уповільнює бізнес, зменшує прибуток і означає, що потрібно шукати більш розумний підхід. Впровадити блокчейн.

Література:

1. *https://www.amd.com/ru/technologies/blockchain*
2. *https://www.ibm.com/ru-ru/blockchain/what-is-blockchain*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Гнядий Владислав Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Сучасний світ сповнений усіляких новинок: науки, техніки, медицини. Ніколи, напевно, люди не володіли такою сумою знань в різних областях. Дивовижні речі і явища оточують нас. Сьогодні можна дістати з кишені новини, приєднатися до мережі, яка існує тільки в інформаційному полі, передати повідомлення людині, яка за тисячі кілометрів від тебе. Завдяки інформаційним технологіям ми можемо знайомитися з людьми, що живуть далеко-далеко, зовсім в інших країнах і містах.

Наука придумала масу цікавого і корисного. Від біоматеріалів до штучної руки. Від швидкісних літаків до швидкісних електричок, що економлять час.

Від електронних бібліотек, онлайн-університетів і курсів до просунутих установок глибокого буріння земної кори. Сучасні технології покликані служити людству, допомагати йому досягати ще більших висот.

Технології, створені найталановитішими людьми, можуть приносити користь, а можуть і шкоду, дивлячись як ними користуватися. За допомогою смартфона, наприклад, можна розводити плітки. Можна не вилазити добами з комп’ютерних стрілялок. Кожною технологією треба користуватися з розумом і розумінням її справжньої користі.

Сучасне матеріальне виробництво та інші сфери діяльності дедалі більше потребують інформаційного обслуговування, перероблювання величезної кількості інформації. Універсальним технічним засобом обробки будь-якої інформації є комп'ютер, що грає роль підсилювача

інтелектуальних можливостей людини і суспільства загалом, а комунікаційні кошти, які використовують комп'ютери, служать для зв'язку й передачі. Поява та розвиток комп'ютерів — це необхідна складова процесу інформатизації суспільства.

Інформатизація суспільства є одним із закономірностей сучасного соціального прогресу. Цей термін дедалі більше витісняє широко використовуваний донедавна термін «комп'ютеризація суспільства». При зовнішній схожості цих понять вони теж мають велику різницю. При комп'ютеризації суспільства основну увагу приділяють розвитку та впровадження технічної бази комп'ютерів, які забезпечують оперативне отримання результатів переробки інформації та її накопичення.

При інформатизації суспільства основну увагу приділяють комплексу заходів, вкладених у забезпечення повного використання достовірного, вичерпного та необхідність своєчасного знання в усіх проявах людської діяльності.

Отже, «інформатизація суспільства» є ширшим поняттям, ніж «комп'ютеризація суспільства», що означає швидше опанування інформації для задоволення власних потреб. У понятті «інформатизація суспільства» акцент треба робити не так на технічних засобах, як на суті доповнень технічного прогресу. Комп'ютери є базовою технічною складовою процесу інформатизації суспільства.

Сучасне суспільство навряд чи можна уявити без інформаційних технологій. Перспективи розвитку обчислювальної техніки сьогодні важко уявити навіть фахівцям. Проте, зрозуміло, у майбутньому очікується щось грандіозне. Якщо темпи розвитку інформаційних технологій не скоротяться (і в цьому немає сумнівів), то дуже швидко.

З розвитком інформаційних технологій зростає прозорість світу, швидкість та обсяги передачі між елементами світової системи. Інформаційні технології увібрали у собі лавинообразне досягнення електроніки і навіть математики, філософії, психології та економіки.

Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки. Тому без інформаційних технологій, як і без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати неспроможне.

Література:

1. *http://bukvar.su/informatika_programmirovanie/169612-Sovremennye-informacionnye-tehnologii.html,*
2. *https://moyaosvita.com.ua/literatura/tvir-na-temu-suchasni-texnologi%D1%97/,*
3. *Хомишин І.Ю. Сучасні інформаційні технології в освіті*

АДМІНІСТРУВАННЯ БЕЗДРОТОВОГО СЕРВЕРА

Голубов Ігор Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У даній статті розглядається питання особливостей адміністрування мереж у сучасному світі. Віддалене адміністрування мережі знаходять широке застосування. Наприклад, для розв'язання проблем, зметою своєчасного прийняття запобіжних мір, що в свою чергу дає змогу не допустити розвиток подій по найгіршому сценарію. Сектор адміністративного програмного забезпечення вже декілька років як вступив у стадію зрілості.
У статті розглянуться адміністрування бездротових комьютерних мереж та базові концепції щодо їх управління.

Вступ

Адміністрування комп'ютерних мереж ніколи не займали домінуючих позицій в IT технологіях. Традиційно незначна роль, що їм відводилась, призвела до того, що структура і функції ПЗ даного класу виявилися в прямій залежності від архітектури обчислюванних систем і еволюціонували разом із ними.

Як відомо, на початку 90-х років ері безроздільного панування хост-комп'ютерів прийшов кінець. Бурхливе поширення розподілених архітектур клієнт-сервер призвело до кардинальних зімни й у сфері керування інформаційними системами. Основна проблема полягала в тому, що адміністраторам довелося мати справу з небаченим раніше різноманіттям ресурсів: різні комп'ютерні платформи, активні мережеві устаткування, та програмні засоби. Ця гетерогенність зажадала рішення цілком нових адміністративних задач - управління розподіленими ресурсаим, електронним поширенням ПЗ, аналіз трафіка і керування пропускною спроможністю мережі, перерозподіли серверного навантаження, відслідковування стану окремих настільних систем і т.д. Справа ускладнювалася ще і тим, що в нове середовище неможливо було перенести додатки адміністрування, що функціонували на мейнфреймах, так що виробникам довелося створювати керуюче ПЗ практично з нуля.

З погляду розв'язуваних задач, у період, коли мейнфрейми знаходилися в зеніті слави, їхнє адміністрування можна було з повною підставою віднести до категорії системного, що не в останню чергу означало існування єдиної уяви обчислювального середовища. Поява розподілених архітектур у якомусь змісті відкинуло всю індустрію адміністрування тому, оскільки на початку цієї епохи задача керування обмежувалися

контролем за функціонуванням окремих компонентів (мережного устаткування, персональних комп'ютерів і робочих станцій, запам'ятовуючих пристроїв, периферії та ін.), причому в багатьох випадках справа зводилася до простого збору даних про ресурси замість справжнього керування їхньою роботою.

Одночасно був зроблений перехід від управління функціонуванням окремих пристроїв до аналізу трафіка в окремих ділянках мережі, керування її логічною конфігурацією і конкретними робочими параметрами, причому всі ці операції можна було виконувати з однієї керуючої консолі. Якщо слідувати траєкторії історичного розвитку засобів адміністрування, то наступний крок полягав у реалізації функцій управління інформаційними системами в цілому, а це означало, що в перелік контрольованих об'єктів додалися мережні операційні системи, розподілені бази даних і сховища даних, додатки і, нарешті, самі користувачі. Нові проблеми, що виникли в розподілених середовищах, призвели до того, що на якийсь час мережне управління стало розглядатися в якості головної турботи адміністраторів інформаційних систем.

Системне ж адміністрування при цьому як би відійшло на другий план, а відповідний інструментарій фігурував у якості автономних служб, чужих стосовно платформ і додатків мережного управління. Ця інверсія, що не цілком відповідає логіці функціонування корпоративних інформаційних систем (оскільки мережа відіграє роль лише допоміжної інфраструктури), зберігалася протягом декількох років. Ситуація змінилася ще раз після того, як кількість розподілених додатків, і насамперед баз даних, функціонуючих у мережі, перейшло за деяке граничне значення. Зростання ролі системного адміністрування в такій ситуації було цілком природним.

Неминучим виявився й інший процес - інтеграція системного і мережного адміністрування, що змусила провідних виробників терміново модернізувати свої продукти. Проте і тут не обійшлося без перегинів: мережне адміністрування часом стало розглядатися як одна з множини складових частин системного адміністрування, а мережа - як один із керованих ресурсів поряд із комп'ютерами, периферійними пристроями, базами даних, додатками і т.д.

Основна частина

Бездротові мережі. Безпровідного середовища поступово входить в наше життя. Як тільки технологія остаточно сформується, виробники запропонують широкий вибір продукції за прийнятними цінами, що призведе і до зростання

попиту на неї, і до збільшення обсягу продажів. У свою чергу це викличе подальше вдосконалення і розвиток бездротового середовища [3, с.15-45].

Труднощі встановлення кабелю - фактор, якій дає бездротової середовищі незаперечну перевагу. Вона може виявитися особливо корисною в наступних ситуаціях:

- в приміщення, сильно заповнених людьми;
- для людей, які не працюють на одному місці;
- в ізольованих приміщеннях і будівлях;
- в приміщеннях, планування яких часто змінюється;
- в будівлях, де прокладати кабель недозволено.

Бездротові з'єднання використовуються для передачі даних в ЛВС, розширених ЛВС і мобільних мережах. Типова бездротова мережа працює так само, як і кабельна мережа. Плата бездротового адаптера з трансівером встановлена в кожному комп'ютері, і користувачі працюють так, ніби їх комп'ютери з'єднані кабелем.

Бездротова мережа використовує інфрачервоне випромінювання, лазер, радіопередачу у вузькому і розсіяному спектрі. Додатковий метод - зв'язок «точка-точка», при якому обмін даними здійснюється тільки між двома комп'ютерами, а не між декількома комп'ютерами і периферійними пристроями**.**

Плати мережевого адаптера. Плати мережевого адаптера - це інтерфейс між комп'ютером і мережним кабелем. В обов'язки плати мережевого адаптера входить підготовка, передача і управління даними в мережі. Для підготовки даних до передачі по мережі плата використовує трансивер, який переформатує дані з паралельної форми в послідовну. Кожна плата має унікальний мережеву адресу.

Плати мережевого адаптера відрізняються рядом параметрів, які повинні бути правильно налаштовані. У їх число входить: переривання (IRQ), адреса базового порту вводу / виводу і базова адреса пам'яті.

Щоб забезпечити сумісність комп'ютера і мережі, плата мережевого адаптера повинна, по-перше, відповідати архітектурі шини даних комп'ютера і, по-друге, мати необхідний тип з'єднувача з мережевим кабелем.

Плата мережного адаптера значно впливає на продуктивність всієї мережі. Існує кілька способів збільшити цю продуктивність. Деякі плати мають додатковими можливостями. До їх числа, наприклад, відноситься: прямий доступ до пам'яті, колективна пам'ять адаптера, колективна системна пам'ять, управління шиною. Продуктивність мережі можна підвищити також за допомогою буферизації або

вбудованого мікропроцесора. Розроблено спеціалізовані плати мережевого адаптера, наприклад, для бездротових мереж і бездискових робочих станцій.

Мережне адміністрування. Якщо не вдаватися в деталі, то задачі, розв'язувані в даній області, розбиваються на дві групи: контроль за роботою мережного устаткування й управління функціонуванням мережі в цілому. У першому випадку мова йде про моніторинг окремих мережних пристроїв (концентраторів, комутаторів, маршрутизаторів, серверів доступу й ін.), настроюванню і зміні їхньої конфігурації, усуненні виникаючих збоїв. Ця достатньо традиційна група задач одержала назву реактивного адміністрування (reactive management) [2, с.29-35].

Друга група націлена на моніторинг мережного трафіка, виявлення тенденцій його зміни й аналіз подій із метою реалізації схем пріоритеризації для забезпечення максимальної пропускної спроможності (proactive management). Сюди ж відноситься задача внесення змін у конфігурацію мережі, управління IP-адресами користувачів, фільтрація пакетів в цілях забезпечення інформаційної безпеки і ряд інших задач. Потреба в контролі за мережею в цілому з однієї керуючої станції стала причиною появи різних архітектур платформ і додатків адміністрування.

Найбільше поширення серед них набула двохрівнева розподілена архітектура “менеджер–агенти”. Програма-менеджер функціонує на керуючій консолі, постійно взаємодіє з модулями-агентами, що запускаються в окремих пристроях мережі. На агенти в такій схемі покладаються функції збору локальних даних про параметри роботи контрольованого ресурсу, внесення змін у його конфігурацію по запиті від менеджера, надання останньому адміністративної інформації.

Незважаючи на очевидні зручності двохрівневої архітектури, її застосування в реальному мережевому середовищі призводить до зростання обсягів службового трафіка і, як наслідок, до зниження пропускної спроможності, доступної додаткам. Цей ефект особливо замітний у складних сегментованних мережах, що містять велику кількість активних пристроїв. У якості часткового рішення проблеми вичерпання пропускної спроможності була запропонована трьохрівнева архітектура, у якій частина керуючих функцій делегувалася найважливішим мережним вузлам. Інстальовані в цих вузлах програми-менеджери через власну мережу агентів управляють роботою “підзвітних” їм пристроїв і в той же час самі виступають у ролі агентів стосовно основної програми-

менеджера (менеджеру менеджерів), запущеної на керуючій станції. У результаті основна частина службового трафіка надається локалізованим в окремих мережних сегментах менеджерам, оскільки «спілкування» локальних менеджерів з адміністративною консоллю здійснюється тільки тоді, коли в цьому дійсно виникає необхідність.

Необхідність контролювати роботу різноманітного устаткування в гетерогенному середовищі зажадала уніфікації основних керуючих процедур. Згадана схема «менеджер - агенти» знайшла вираження в протоколі Simple Network Management Protocol (SNMP), що швидко став базовим протоколом мережевого адміністрування, і в стандарті дистанційного моніторингу RMON. Управління настільними системами звичайно здійснюється на базі стандарту Desktop Management Interface (DMI), розробленого організацією Desktop Management Task Force (DMTF).

Результат такого розвитку подій неважко передбачити наперед: індустрія ПЗ мережневого управління виявилася розділеною на три частини. Першу утворюють платформи мережного управління - аналоги операційних систем, що формують середовище для запуску додатків, але при цьому вони володіють обмеженою функціональністю. Друга група мережевих програм пов'язана з керуючими додатками виробників мережних апаратних засобів. Проте вони розраховані на управління тільки визначеною групою пристроїв і рідко дозволяють обслуговувати вироби інших компаній. Подібні додатки пропонуються практично усіма відомими постачальниками устаткування. Третя група - численні програми третіх фірм, націлені на рішення вузьких задач мережного адміністрування.

Програми для віддаленого адміністрування

У обов'язки адміністратора мережі можуть входити задачі, пов'язані з адмініструванням робочих станцій і управлінням ними з метою підтримки їх в оптимальному стані для роботи в мережі. В цьому випадку для кожного користувача необхідно надати певні права доступу, дозволяючи, або забороняючи їм вносити зміни в систему. А якщо такі зміни і були внесені то при наступному завантаженні ці зміни повинні бути відмінені. Наскільки жорстким повинен бути контроль за конфігурацією робочих станцій, визначається адміністратором мережі. Тому для полегшення роботи системних адміністраторів були створені програми віддаленого управління робочими станціями, що можуть бути використані і для управління серверами. Можливість віддаленого управління і адміністрування підвищує

оперативність усунення проблем, які можуть виникнути в мережі. Колись програми для віддаленого адміністрування були потрібні тільки на підприємствах, де одній людині доводиться обслуговувати десятки, а то і сотні комп'ютерів, які розташовані в різних кабінетах і на різних поверхах. Сьогодні сфера їх застосування набагато ширша [1, с.292-295].

По-перше, в багатьох квартирах більше одного комп'ютера, і між ними для швидшої передачі інформації протягнута мережа. Якщо комп'ютери стоять в різних кімнатах, то програма для віддаленого адміністрування дає можливість працювати на двох ПК одночасно, не встаючи із стільця.

По-друге, як правило, люди постійно працюють з двома комп'ютерами - домашнім і робочим. Програми для віддаленого адміністрування дозволяють через Інтернет стежити за тим, що відбувається на іншому комп'ютері. Одним словом, програма для віддаленого адміністрування просто необхідна кожному, в чиєму розпорядженні знаходиться більше одного комп'ютера.

Більшість програм для віддаленого адміністрування складається з двох частин - серверу і клієнта (його ще називають “вьювер”, або “просмотрщик”). Перший встановлюється на віддаленій машині, тобто, на тій, якій потрібно управляти. Клієнтська частина ставиться на комп'ютері, з якого ви плануєте управляти іншим ПК. Для того, щоб клієнт працював, на віддаленому ПК обов'язково повинна бути запущена серверна частина, тому при установці на віддаленому ПК програму краще відразу помістити в "Автозавантаження". Окрім цього, якщо на комп'ютерах використовується брандмауер, потрібно обов'язково створити правило, що дозволяє роботу з додатками для віддаленого адміністрування, інакше брандмауер може вирішити, що підключення до ПК - це атака ззовні і не допустити підключення [4].

Висновки

У даній статті було розглянуто особливості адміністрування компьютерних мереж.

З розвитком інформаційних технологій зокрема інформаційних систем змінилися базові концепції щодо їх управління - мережне і системне адміністрування інтегрували в єдиний комплексний підхід.

Аналіз розвитку комерційних програм мережного і системного адміністрування дозволяє зробити висновок, що ідея адміністрування зводиться до аналізу поводження інформаційної системи, або окремих її компонентів зметою своєчасного прийняття запобіжних мір, що в свою чергу дає змогу не допустити розвиток подій по найгіршому сценарію.

Сектор адміністративного програмного забезпечення вже декілька років як вступив у стадію зрілості. На ринку є широка гама пропозицій - від базових платформ до оптимізованих засибів для виконання широкого кола задач. Більше того, якщо розглядати засоби адміністрування найбільших виробників, то розходження між ними в плані функціональності стають усе більш розмитими, що надає користувачам додаткову свободу вибору.

Література:

1. Computer Vision Applications: How Real-Time Image Processing is Reshaping Industries and How Your Business Can Leverage It [Електронний ресурс] – Режим доступу до ресурсу: https://perfectial.com/blog/computer-vision-applications/.

2. Aggarwal C. Neural Networks and Deep Learning / Charu C. Aggarwal. – Yorktown Heights, USA: Springer International Publishing AG, 2018. – 512 p.

3. Top 6 Deep Learning Models You Should Master for Killer AI Applications [Електронний ресурс] – Режим доступу до ресурсу: https://towardsdatascience.com/top-6-deep-learning-models-you-should-master-for-killer-ai-applications-13c7dfa68a3.

ТОП 5-ТЕХНОЛОГІЙ МАЙБУТНЬОГО, ЩО ПІДКОРИЛИ СВІТ

Голюк Дмитро Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Казкове майбутнє: літаючі машини, роботи-люди, будинки з голосовим управлінням, власні віртуальні помічники, їжа «з повітря» і надруковані на принтері людські органи. Розповідаємо про найнеймовірніших технологіях, які вже втілилися в життя. Як часто в дитинстві ви читали книги, дивилися фільми або мультфільми про майбутнє і думали про те, що людство ніколи не винайде літаючий скейт, складаний смартфон або робота, який би повністю був схожий на людину?

Якими будуть повсякденні речі, які нас оточують, через кілька років? Деякі концептуальні технології, які розробляються вже зараз, дозволяють зазирнути в майбутнє і уявити, чого від нього можна очікувати.

1. Розумне скло

Міцне, гнучке, розумне … скло? Так, ми, можливо, того не помічаючи, входимо в «еру скла».Володіючи можливістю ставати прозорим і непрозорим, залишатися міцним і небитким і навіть вести себе як сенсорна панель, новий тип скла зможе змінити наші домівки і робочі місця до невпізнання.Стіни в таких будинках при бажанні зможуть вести себе як вікна, контролюючи обсяг пропускається ультрафіолетового випромінювання, тепла і роблячи наші оселі і транспорт набагато енергоефективніше. Тільки уявіть, що кожна поверхню

вашого будинку буде здатна трансформуватися з стіни в вікно, а з вікна в екран телевізора просто по руху вашої руки. Подібні технології по-справжньому ваблять.

2. Штучний інтелект

Вже довгий час ЗМІ обіцяють нам майбутнє, в якому ми зможемо спілкуватися з кібернетичними напарниками, здатними розуміти наші команди і запити, емоції і навіть гумор. Однак в нинішньому світі ця мрія так поки і залишається мрією. І все ж щодо скоро все може змінитися, так як інженери в поті чола працюють над створенням програми, яка по-справжньому буде здатна розуміти людські емоції і вираження. Завдяки передовим досягненням в технологіях лицьового розпізнавання, деякі існуючі програми вже здатні розуміти, коли ви злитеся або сумуєте, а деякі навіть здатні описувати ті події, які вони «бачать». Все це перші кроки до створення роботів, які будуть наділені можливістю розпізнавати і описувати світ навколо них, а потім ділитися своїм досвідом з нами. Саме дотримуючись цієї ідеї, вчені сподіваються, що одного разу зможуть поділитися цим світом з емоційно дорослими і розважливими машинами.

3. Аугментація людей

Біоніка змінює обличчя людства. У буквальному сенсі. Чим більше ми стаємо залежними від машин, тим швидше ми наближаємося до часу, коли наші можливості стануть на порядок вище і ширше, ніж ті, якими ми володіємо сьогодні. Імплантація відеокамер в очі, поліпшення здатності вище стрибати і швидше бігати, або ж навіть контролювання електронних пристроїв силами нашого розуму – межа між машиною і людиною повільно, але вірно стає все більш розмитою. Завдяки новим можливостям ми, найімовірніше, зможемо навіть відчути і отримати абсолютно незнайомий для нас до цього досвід. Може, ми зможемо «чути» кольору або «відчувати» електричні поля або навіть завантажувати нову інформацію в наш мозок, як фільмі «Матриця».

4. Голограми

Проектування будинків. Відеоігри. Дослідження космосу. Будівництво нових світів. І все це в тривимірному просторі. Саме таке майбутнє обіцяють нам голографічні технології. Здатна доповнити наш фізичний світ цифровим, ця технологія має величезний потенціал практично у всіх відомих нам сферах. Малювати в повітрі, ходити по поверхні Марса, заглянути в жерло вулкана і центр Землі – голограми можуть відправити нас туди, куди навіть магія, не те що наука, не спроможна. Можливості будуть практично безмежні і прямо залежати лише

від нашої уяви. Хто знає, що ще тільки зможуть створити люди за допомогою цієї технології.

5. Спритні роботи

Промислові роботи все ще незграбні. Робот може неодноразово і з вражаючою точністю підбирати компоненти на конвеєрі. Він не занудьгує від монотонної роботи – але якщо ви перемістите об'єкт на сантиметр, або заміните чимось дещо іншим – дії машини будуть нечіткими, чи вона просто промахнеться. Хоча робот ще не може бути запрограмованими на те, щоб зрозуміти як взяти будь-який об'єкт, просто дивлячись на нього, як це роблять люди, він тепер може навчитися маніпулювати об'єктом самостійно за допомогою системи віртуальних проб і помилок.

Література:
1.Журнал Technology Review Массачусетського технологічного інституту
2.звіт Global Industry Vision від Huawei

ЩО МОЖУТЬ НАНОТЕХНОЛОГІЇ: 10 СПОСОБІВ ЗАСТОСУВАННЯ ТА ВАЖЛИВІСТЬ ДЛЯ СУСПІЛЬСТВА

Голюк Дмитро Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Нанотехнології є загальновживаним словом у наші дні, але ж що можуть нанотехнології? Багато хто з нас не усвідомлюють, який надзвичайний вплив вони можуть зробити на наше повсякденне життя. Згідно з Національною ініціативою нанотехнологій США, нанотехнологія – це "наука, техніка та технології, що проводяться на нанорівні, тобто приблизно це становить від 1 до 100 нанометрів". Один нанометр – це мільярдна частина метра. Для порівняння, аркуш газети має товщину близько 100 000 нанометрів.

Це також галузь, що швидко розширюється. Вчені та інженери мають великий успіх у вивченні того, що можуть нанотехнології та створенні матеріалів на наномасштабі, щоб скористатися розширеними властивостями, такими як більша міцність, легша вага, підвищена електропровідність та хімічна реакційна здатність порівняно з їх великими еквівалентами.

Нижче наведено 10 способів щоденного впливу нанотехнологій на наше життя.

Що можуть нанотехнології?

1. Швидші, менші та потужніші комп'ютери, які споживають набагато менше енергії, з батареями, що працюють довше. Схеми, виготовлені з вуглецевих нанотрубок, можуть

мати життєво важливе значення для підтримання зростання потужності комп'ютера.

2. Швидше, функціональніше та точніше медичне діагностичне обладнання. Технологія Lab-on-a-chip дозволяє проводити тестування в режимі реального часу, що прискорює надання медичної допомоги. Наноматеріальні поверхні на імплантатах покращують знос та протистоять зараженню.

3. Наночастинки у фармацевтичних продуктах покращують їх всмоктування в організмі та полегшують їх доставку, часто за допомогою комбінованих медичних виробів. Наночастинки також можуть використовуватися для доставки хіміотерапевтичних препаратів до певних клітин, таких як ракові клітини.

4. Поліпшення паливної ефективності автомобіля та стійкості до корозії шляхом створення деталей автомобіля з нанокомпозитних матеріалів, які легші, міцніші та хімічно стійкіші, ніж метал. Нанофільтри видаляють з повітря майже всі частинки, що потрапляють у повітря, до того, як воно потрапить у камеру згоряння – більше покращуючи пробіг газу.

5. Наночастинки або нановолокна в тканинах можуть підвищити стійкість до плям, водонепроникність і вогнестійкість без значного збільшення ваги, товщини або жорсткості тканини. Наприклад, «нановусики» на штанах роблять їх стійкими до води та плям.

6. Фільтри для води шириною лише 15-20 нанометрів можуть видаляти наночастинки, включаючи практично всі віруси та бактерії. Ці економічно вигідні портативні системи очищення води ідеально підходять для поліпшення якості питної води в країнах, що розвиваються.

7. Вуглецеві нанотрубки мають різноманітні комерційні цілі, зокрема роблять спортивне обладнання міцнішим та легшим. Наприклад, тенісна ракетка, виготовлена з вуглецевих нанотрубок, менше прогинається під час удару та збільшує силу та точність подачі. Наночастинки, якими оброблені тенісні мячі, можуть допомогти їм стрибати вдвічі довше, ніж стандартні тенісні м'ячі.

8. Сьогодні більшість сонцезахисних кремів виготовляються з наночастинок, які ефективно поглинають світло, включаючи більш небезпечний ультрафіолетовий діапазон. Вони також легше поширюються по шкірі. Ці самі наночастинки також використовуються в упаковці харчових продуктів, щоб зменшити вплив УФ та продовжити термін зберігання.

9. Багато пляшок для напоїв виготовляються з пластмас, що містять наноглини, які підвищують стійкість до проникнення кисню, вуглекислого газу та вологи. Це допомагає утримувати карбонізацію та тиск і збільшує термін зберігання на кілька місяців.

10. Завдяки нанотехнологіям можна запрограмувати величезну кількість різноманітних хімічних датчиків для виявлення певної хімічної речовини на дивовижно низьких рівнях, наприклад, однієї молекули з мільярдів.

Література:
1. https://www.asme.org
2. https://futurenow.com.ua

ПОКРАЩЕННЯ СИСТЕМИ НАВЧАЛЬНОГО ПРОЦЕСУ ЗА ДОПОМОГОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Голюк Дмитро Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Навчання з використанням інноваційних технологій якісно перевищує класичну освіту. Воно інтегрує процеси, які не можна об'єднувати в межах класичної освіти. Сучасне суспільство характеризується швидкими змінами в усіх сферах життя, що особливо впливає на розвиток інформаційного, зокрема й освітянського простору. Освітня сфера, яка є основоположницею формування світогляду, духовного становлення особистості, зазнає значних трансформаційних процесів. Простір, де стикаються нові цінності й технології, нові стилі життя, вимагає нових, сучасних освітніх підходів. Гуманізація освіти, її орієнтація на розкриття особистісного потенціалу зумовили виникнення й удосконалення нових освітніх технологій.Тому вимогою сьогодення стає апробація й упровадження інноваційних освітніх технологій у навчально-виховний процес.

Національна стратегія розвитку освіти в Україні на період до 2021 року визначає запровадження освітніх інновацій як один із пріоритетних напрямів державної політики в освітній сфері.

В умовах інформаційного суспільства традиційне навчання поступово втрачає свій сенс. Величезний потік інформації, яка старіє швидше, ніж студент закінчує навчальний заклад, вже не можливо вмістити до навчальної програми. Втрачає сенс необхідність перенавантажувати пам'ять дитини додатковими знаннями, необхідно навчати дитину знаходити їх і користуватися ними. Тому дієвим інструментом поліпшення якості освіти визначають застосування компетентнісного підходу до освіти, який на перше місце ставить не поінформованість студента, а вміння на основі знань розв'язувати проблеми, які виникають у різних ситуаціях. Щоб

навчити цього потрібно змінити технологію навчального процесу. Поняття "Інформаційні технології навчання" виникло у сімдесяті роки і передбачало організацію навчального процесу на базі паперових (книги, друковані матеріали тощо) та плівкових (фото, діапозитиви, кіно-матеріали) носіїв інформації. На сучасному етапі інформаційні технології набули нового розвитку. Це пояснюється масовим застосуванням у навчальному процесі персональних комп'ютерів та комп'ютерних систем. Інформатизація освіти являє собою комплекс заходів, пов'язаних із використанням інформаційних засобів та інформаційної продукції.

До складу інформаційної технології входить:

1. Технічне середовище, яке являє собою вид використовуваної техніки для розв'язку основних завдань.

2. Програмне середовище, яке створює набір програмних засобів.

3. Предметне середовище, яке визначає зміст конкретної науки на рівні навчальної дисципліни.

4. Методичне середовище, яке передбачає наявність інструкцій, порядку застосування, оцінки ефективності тощо.

Інформаційні технології навчання перш за все обумовлюються використанням навчальних засобів як спеціально розроблених матеріальних чи матеріалізованих об'єктів, застосування яких спрямоване на забезпечення ефективності навчального процесу. Найяскравіше сучасні інформаційні програми навчання представлені в комп'ютерних технологіях. Комп'ютерні технології обумовлюються психологічними, логічними, змістовими, організаційними аспектами. Цілеспрямоване, обґрунтоване, систематичне застосування комп'ютерних програм забезпечує розв'язок інформаційних, навчальних, контрольних та організаційних функцій.

Технологічне використання комп'ютера в навчальному процесі розв'язує ряд проблем:

1. Освітню: знайомлять студентів з можливостями обчислювальної техніки; прищеплюють їм уміння та навички доцільного її використання; формує уміння користуватись навчальними програмами.

2. Педагогічну: допомагає студентові швидко і якісно засвоювати навчальний матеріал; унаочнює навчальний процес; індивідуалізує навчання.

3. Організаційну: забезпечує можливість одночасного комп'ютерного тестування усіх студентів; проводить комп'ютерний контроль за якістю роботи та її економний облік.

Інформатизація освіти створює передумови для широкого впровадження в практику психолого-педагогічних розробок, які забезпечують ряд аспектів. Обчислювальна техніка, яка увійшла в усі сфери людського життя, створює все нові форми людської діяльності, як окремого індивіда, так і в цілому всього нашого суспільства. Саме цей чинник значною мірою впливає на психологію людини (когнітивна, операційно-технічна сфери, мотивації, здібності).

Зрозуміло, якщо такий вплив на психіку людини не враховувати при використанні комп'ютерів у процесі навчання, розробці програмних продуктів, то це може негативно відбитись на розвитку особистості. Деякі психологи відзначають, що в нашому житті техніки і новітніх інформаційних технологій слід говорити не тільки про соціальні, а й актуальні теми психологічних наслідків комп'ютеризації.

Відомий психолог О. Тихомиров виділяє такі психологічні проблеми застосування ЕОМ, які необхідно враховувати:

– вплив інформатики, обчислювальної техніки, засобів автоматизації на психіку людини;

– вплив їх на психологічну науку, що вивчає закони психічного життя;

– використання наукових психологічних знань у працях з інформатики та обчислювальної техніки.

Вчений визначає комп'ютеризацію та мету її впровадження як вимогу часу. Використання техніки викликане суспільними проблемами і, безперечно, за допомогою психологічної науки можна досягти кращого результату. Так як і при комп'ютеризації в першу чергу йдеться про людину та суспільство, а це – пріоритетні напрямки психології.

Література:

1. Гуревич Р.С, Кадемія М.Ю. Інформаційно-комунікаційні технології у навчальному процесі: посібник для педагогічних працівників і студентів педагогічних вищих навчальних закладів. – Вінниця: ДОВ "Вінниця", 2002. –116 с. 2. Сучасні інформаційні засоби навчанням Навчальний посібник / ПК. Р.С. Гуревич, Л.Л. Коношевський, О.В. Шестопалюк. – Вінниця: ВДПУ імені Михайла Коцюбинського, 2004. – 535 с

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Грабовий Вадим Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

В даний період історії людство переживає науково-технічну революцію, в основі якої стоїть електронно-обчислювальна техніка. В результаті, на базі цієї техніки з'являється новий вид технологій – інформаційні. До них належать

процеси, де вхідною «сировиною» та готовим «продуктом» виступає інформація. Головну роль в інформаційних технологіях грає інформація, а не те, де вона оброблюється. Як виробничі, так і інформаційні технології виникають не спонтанно, а в результаті технологізації(інформатизації) того чи іншого соціального процесу, тобто цілеспрямованого активного впливу людини на ту чи іншу область виробництва і перетворення її на базі машинної техніки [1].

Ключові слова: науково-технічна революція, електронно-обчислювальна техніка, інформація, інформаційні технології, інформатизація.

Сучасна людина не може уявити своє життя без таких, раніше навіть здавалося – неймовірних, речей як телефон, телевізор, радіо, а головне – без комп'ютера. Але світ не стоїть на місці і тому не обхідно йти, як кажуть, «в ногу часом». Для більшості людей комп'ютер став їхнім другим життям, в якому вони можуть вільно спілкуватися з людьми з різних куточків світу, слухати музику, дізнаватися корисну інформацію, дивитись фільми та серіали. Це все можна назвати одним словом – інформатизація. Інформатизацією суспільства називають глобальний соціальний процес, при якому домінуючим видом соціальної діяльності є збір, накопичення, продукування, обробка, зберігання, передача та використання інформації, які здійснюються на основі сучасних засобів мікропроцесорної та обчислювальної техніки [2].

Для удосконалення механізмів управління суспільним ладом, сприянню гуманізації і демократизації суспільства, а також підвищення рівня добробуту його членів, необхідне застосування відкритих інформаційних систем, розрахованих на використання всього масиву інформації, доступної в даний момент суспільству в певній його сфері. Сучасні інформаційні технології вмістили в себе величезні досягнення електроніки, а також математики, психології, філософії та економіки. В результаті чого був утворений життєздатний гібрид, який ознаменував революційний стрибок в історії інформаційних технологій, який налічує сотні тисяч років. Сучасне суспільство буквально пронизане потоками інформації, які потребують обробки, і тому без інформаційних технологій, так само як без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати не може [3].

Відповідно до визначення з Енциклопедії сучасної України, Інформаційні технології [4] – це сукупність методів, програмно-технічних і технологічних засобів, що забезпечують той самий вид роботи з інформацією, що і при інформатиації, а також автоматизацію керування бізнес-процесами організацій, проектування та виробництва устаткування. Відповідно до визначення можна виділити таких фахівців, які працюють з інформаційними технологіями [5]:

- фахівці, які займаються технічними розробками та обслуговуванням комп'ютерного обладнання;
- фахівці, які займаються створенням ПЗ для різних обчислювальних пристроїв;
- фахівці, які працюють з уже створеними інформаційними продуктами.

Від фахівців із перших двох категорій залежить те, як користувачі будуть передавати та отримувати інформацію. Більш конкретні назви професій цих фахівців – системні адміністратори, програмісти різних профілів, інженери комп'ютерного обладнання, тестувальники програмного забезпечення, фахівці з інформаційної безпеки.

До видів сучасних інформаційних технологій можна віднести [3]:

- інформаційна технологія опрацювання даних;
- інформаційна технологія керування;
- інформаційна технологія підтримки прийняття рішень;
- інформаційна технологія експертних систем.

Україна за рівнем розвитку інформаційних технологій у світі посідає 56 місце (2016; Всесвітній економічний форум у своїй шостій щорічній доповіді). У попередньому рейтингу Україна займала 71 позицію. Єдина конкурентна перевага, яку має Україна в цьому аспекті, це традиційно сильні IT-кадри, тобто в Україні дуже високий рівень підготовки програмістів. Україна є одним зі світових центрів офшорного програмування [1].

У складеному рейтингу лідирує Данія — завдяки зразковій нормативно-правовій базі і чіткій політиці держави з поширення інформаційних технологій. Друге місце зайняла Швеція, яка за 2006 рік піднялася на шість позицій, ставши однією з країн із найбільшим ростом IT —сектору економіки. Також у першу трійку потрапив Сінгапур. У першу десятку увійшли Фінляндія, Швейцарія, Нідерланди, США, Ісландія, Велика Британія та Норвегія. 2009 року KPMG внесла Львів у список 30 міст світу з найбільшим потенціалом розвитку інформаційних технологій [1].

Література:

1. Інформаційні технології [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Інформаційні_технології#:~:text=Україна%20за%20рівнем%20розвитку%20інформаційних,рейтингу%20Україна%20займала%2071%20позицію.

2. Сучасні інформаційні технології поняття, структура, технології [Електронний ресурс] – Режим доступу до ресурсу: https://works.doklad.ru/view/GRx9bTCcRpY.html.

3. Сучасні інформаційні технології і Україна [Електронний ресурс] – Режим доступу до ресурсу: http://megalib.com.ua/content/2054_91_Sychasni_informaciini_tehnologii_i_Ykraina.html.

4. Енциклопедія сучасної України [Електронний ресурс] – Режим доступу до ресурсу: http://esu.com.ua/search_articles.php?id=12474.

5. Що таке інформаційні технології [Електронний ресурс] – Режим доступу до ресурсу: http://apeps.kpi.ua/shcho-take-informatsiini-technologii/en.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ. ЛЮДИНА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Гридяєва Вероніка Русланівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Сьогодні комп'ютерна грамотність є невід'ємною частиною повсякденного життя і необхідною умовою працевлаштування та успішної кар'єри.

Створення та функціонування інформаційних систем в управлінні тісно пов'язані з розвитком інформаційної технології — головною складовою частини автоматизованої інформаційної системи. Інформаційна система за своїм складом нагадує підприємство з перероблення даних і виробництва вихідної інформації. Як і в будь-якому процесі, в інформаційній системі наявна технологія перетворення даних у результативну інформацію.

Автоматизована інформаційна технологія (АІТ) — системно організована для розв'язання задач управління сукупність методів і засобів реалізації операцій збору, реєстрації, передачі, нагромадження, пошуку, оброблення і захисту інформації на основі застосування програмного забезпечення, засобів обчислювальної техніки та зв'язку, а також засобів, за допомогою яких інформація пропонується клієнтам. Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. На її основі створено та створюються обчислювальні системи й мережі різних конфігурацій не тільки для нагромадження, зберігання, перероблення інформації, але й максимального зближення термінальних улаштувань до робочого місця спеціаліста та для підтримки прийняття рішення керівника.

Основу нової інформаційної технології складають розподілена обчислювальна техніка, «дружнє» програмне забезпечення та сучасні засоби комунікації. Принципова відміна нової інформаційної технології полягає не тільки в автоматизації процесів зміни форми й розміщення інформації, а й у зміні її змісту. І сьогодні можна говорити про забезпечувальні ІТ і функціональні ІТ.

Забезпечувальні ІТ — технології оброблення інформації, які використовуються як інструмент у різних предметних сферах для розв'язання різних задач. Функціональні ІТ — це модифікація забезпечувальних ІТ, за якої реалізується, будь-яка

з предметних технологій. Наприклад, в арсеналі облікового процесу можуть перебувати як забезпечувальні технології (наприклад, текстові й табличні процесори), так і спеціальні функціональні технології (табличні процесори, СУБД, експертні системи, реалізуючі предметні технології).

Інформаційні технології можна класифікувати за рядом ознак:

- за способом реалізації в АІС;
- за ступенем охоплення задач управління;
- за класом реалізуючих технологічних операцій;
- за типом користувацького інтерфейсу;
- за способом побудови мережі;
- за обслуговуючими предметними сферами.

Одна з сучасних тенденцій розвитку інформаційних технологій — напрям технології «клієнт—сервер». Цей підхід реалізується в технології зв'язування та запровадження об'єктів (OLE), організації локальних мереж і мережевих операційних систем, у глобальних мережах типу Internet, в архітектурі систем керування базами даних, в архітектурі пакетів прикладних програм.

Двадцять перше століття - століття інформаційних і телекомунікаційних технологій. Отримання пошти через хвилину після відправлення листа, прокладання найбільш оптимального шляху для пересування завдяки інформації з навігаційних пристроїв, віртуальні засоби інформації, соціальні мережі для спілкування, дистанційна освіта, використання ресурсів мережевих бібліотек, віддалена робота в мережі Інтернет. Отримавши простий доступ до мільйонів терабайт знань нам стало простіше розвивати себе в інтелектуальному плані. Ще якихось 20-30 років назад всі ці речі здавалися фантастикою.

У минуле йдуть і готівкові розрахунки. Сьогодні платежі доступні не тільки через інтернет банкінг з рахунків кредитних та розрахункових карт, а й різними видами «інтернет грошей» - мережевими валютами. Вже існують аналітичні медичні комплекси, які здатні самостійно виконувати цілий ряд вимірювань в автоматичному режимі та інтерпретувати дані вимірювань без втручання лікаря, а також передавати інформацію в інформаційну базу лікувальної установи.

Важко, а то й неможливо уявити собі людину, яка прямо або опосередковано не використовує інформаційні технології. Комп'ютери та електронні гаджети міцно увійшли в наше життя і змінили його. Щорічно з'являються і розробляються технологічні новинки, що поліпшують якість повсякденного

життя людини. З появою таких технологій наше життя стало набагато комфортнішим. Розвивається тенденція збільшення багатофункціональності речей, що оточують людину. Мобільні телефони, наприклад, перестали нести свою функцію тільки лише як засоби зв'язку - їх функціонал зріс практично до рівня персональних комп'ютерів. Розробляються гаджети, які здійснюють контроль у режимі реального часу фізіологічних показників людини; системи безпеки, які працюють з персональною інформацією за допомогою дактилоскопічного доступу, датчики, які використовують для відстежування. З'явилися технології «розумний дім» - дистанційного керування інфраструктурою житла. Все більша кількість побутової техніки має вбудований процесор і може з’єднуватися з іншими гаджетами та самостійно задавати алгоритм роботи, наприклад, як це робить робот-пилосос. Але існує й негативний фактор технологічної революції - людина все більш залежна від техніки і технологій та не може фізично і психологічно відмовитися від спокус науково-технічного прогресу.

Очевидно, що новітні комп’ютерні та інформаційні технології, а особливо мережеві суттєво впливають на життєдіяльність людини, але ще більшою мірою цей вплив поширюється безпосередньо на сам мозок, який звикає працювати в інтенсивному режимі багатозадачності.

***Література**:*

1. https://sites.google.com/view/smirnovaseu/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0/10-11-%D0%BA%D0%BB%D0%B0%D1%81/%D0%B1%D0%B0%D0%B7%D0%BE%D0%B2%D0%B8%D0%B9-%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C/%D1%83%D1%80%D0%BE%D0%BA-2-%D0%B1%D0%BC-1

АНАЛІЗ ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ ПОКРАЩЕННОГО МОБІЛЬНОГО ШИРОКОПОЛОСНОГО ЗВ’ЯЗКУ (eMBB) В МЕРЕЖАХ ЗВ’ЯЗКУ П’ЯТОГО ПОКОЛІННЯ

Гуріч Олександр Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій
м. Київ

Стрімкий розвиток сучасних інформаційних технологій в усіх сферах життя, сприяє до появи нових підходів та методів організації мобільного зв’язку. Вже сьогодні створюються на впроваджуються стандарти мереж мобільного зв’язку п’ятого покоління, які створюють базу для створення істотно нової архітектури в сфері надання інформаційних послуг, де однією із

найбільш важливих складових є – надання послуг покращеного мобільного широкополосного зв'язку.

Мережі мобільного зв'язку 5-го покоління – це абсолютно новий підхід до надання інформаційних послуг, оскільки вперше відбувається перехід від надання традиційних сервісів мобільного зв'язку, зокрема голосу, до широкого спектру послуг з різними вимогами до швидкостей, затримки, частотного діапазону та методів передачі сигналу.

Саме тому, послуги, що надаються мережами 5G, були поділені МСЕ на 3 групи:

1. eMBB
2. mMTC
3. URLLC

Предметом даної роботи є вивчення та аналіз першої групи послуг – eMBB.

eMBB - це розширення послуг, що вперше використовувалос в сімействі 4G LTE, що забезпечує високу швидкість передачі даних у широкій зоні покриття. eMBB забезпечує більшу емність, необхідну для підтримки пікових швидкодіючих передач даних як для великих скупчень людей, так і для кінцевих користувачів, які знаходяться в русі. Початкова фаза автономних мереж 5G фокусується на eMBB, що забезпечує більшу полосу передачі даних. Це допоможе розробити сучасні варіанти використання мобільного широкополосного доступу, такі як нові медіа та додатки AR / VR, потокове відео UltraHD або 360-градусна передача та багато іншого.

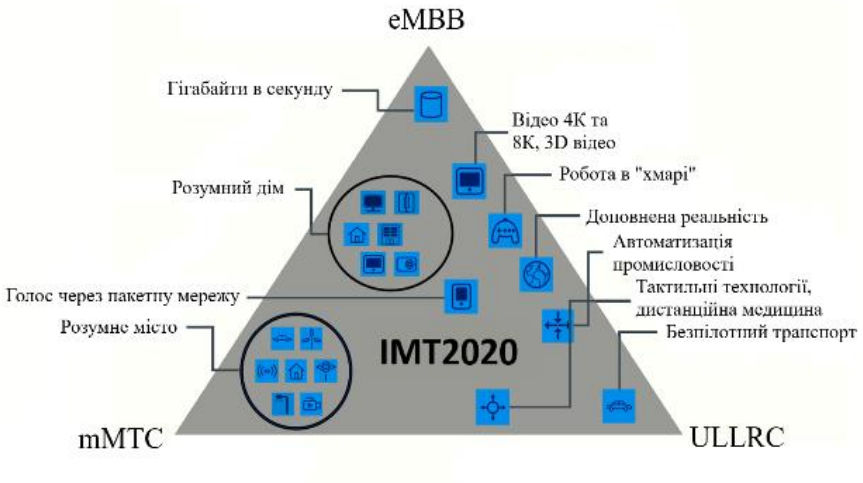


Рис. 1 Послуги, що надаються в мережах 5G

Ця група послуг охоплює сценарії використання, орієнтовані на людину і забезпечують доступ до мультимедійного контенту, послуг та даних (аналогічна послугам, що надаються в даний час мережами LTE). До таких послуг належать: Ultra HD і відео, 3D відео, в тому числі в реальному часі, онлайн ігри, віртуальна реальність (можливі області застосування: освіта, розваги, охорону здоров'я, військова промисловість), розширені сервіси соціальних мереж, хмарні сервіси (можливі області застосування: державні послуги, бізнес додатки, обчислення), голос, в тому числі потоковий, музика в реальному часі, мовлення MBMS.

Для якісної підтримки цих послуг повинні забезпечуватися мультігігабітні швидкості передачі даних. У сценаріях для eMBB високе значення мають практична призначена для користувача швидкість передачі даних, трафік на одиницю площі, пікова швидкість передачі даних, мобільність, енергоефективність та ефективність використання спектра.

Отже, впровадження даного типу мобільного зв'язку в мережах п'ятого покоління відкриває багато можливостей як для звичайних користувачів, так і для операторів телекомунікацій, що позитивно вплине на подальший розвиток інформаційних технологій.

Література:

1. *eMBB URL – https://ru.wikipedia.org/wiki/EMBB*
2. *Услуги 5G URL – http://1234g.ru/5g/uslugi-5g*

IMPROVING THE RELIABILITY OF STORING INFORMATION IN MICROCOMPUTER COMPLEXES OF PERSONAL IDENTIFICATION

Danylchenko Valentyna, Mykolaichuk Vira
Senior Lecturer in the Department of Information Systems and Technologies
State University of Telecommunications
Kyiv

Formulation of the problem

Microcomputer complexes of personal identification (MCPI), built on the basis of technologies RFID (Radio Frequency Identification) and SMART, play an extremely important function, they are carriers of exclusive data of the owner. Vivid representatives of this class are, for example, a bank card, electronic access keys, car chip keys, digital television, a mobile phone SIM card. Obviously, the value of information in MCPI far exceeds its market value. Loss or misrepresentation of information is critical and inadmissible. Thus, long-term storage and timely provision of information is a key

function of every MCPI. There are virtually no publications in the open press about improving the reliability of MCPIs by developing and modifying methods and algorithms for processing, storing and inputting information. These devices do not use algorithms to ensure the integrity of information and reliability, which can cause errors, independent of the actions of the owner.

The aim of the study

It is proposed to consider the decision on application of noise - coding algorithms for SMART and RFID devices, built on electronic integrated circuits, containing, in addition to memory modules - microprocessor with arithmetic - logic device, control device, input - output device, registers [1]. The MCPI assumes the presence of a specialized file system (Chip Operation System, GSM File System), which provides a large set of service operations and security tools and provides for delimiting access to information.

Research results

A permanent storage device (ROM) is used to store the identification data on the memory chip cards. To store other data, including modifiable data, SMART cards and RFID devices use an electrically – alterable read only memory (EAROM). This type of memory, as well as memory ROM is non-volatile, but unlike it in the EAROM can be recorded during chip operation. Consider organizing data storage in the EAROM based on the Hamming and Reed-Solomon codes.

Hamming code $C_H\left(\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1}-m\right)$. The number of *N* pages of the EAROM memory in which the code will be placed will generally not coincide with c $\frac{q^m-1}{q-1}$. But the necessary C code can be constructed by applying to the Hamming code an operation of code shortening [2], which consists in removing several information symbols from the code. The protection of the C_H code from errors is not diminished. In order to be able to obtain the C code from the Hamming C_H code by the shortening operation, the parameter m of the Hamming code must satisfy inequalities.

$$\frac{q^m-1}{q-1} \geq N.$$

Reed-Solomon CRS (q-1, q-2t) codes, unlike the Hamming codes, are generally capable of correcting more than one error and always satisfy the Singleton boundary. In the case of codes that correct $t = 1$ errors, you can also build code words by picking one character from each page of data.

In the case of an arbitrary value of parameter t, it is possible to construct code words in such a way that t characters are taken from each data page and *2t* control characters are placed in the same way

on two control pages. Since the code corrects t errors, any single page memory failure will be corrected. Such use of codes that correct more than one error has the undeniable advantage in terms of correcting errors not related to memory page failure. If more than one error occurs within one code word, such code will deal with it unlike code that corrects one error.

Since a memory page failure can be detected without the use of a decoding procedure, it is performed only after an error is detected. The decoding procedure for computational complexity itself is the same as the encoding procedure. Its algorithm code is also quite compact and can be stored in the memory of a SMART card or RFID tag.

Conclusions and Prospects

Implementations of fault-tolerant coding based on Hamming, Reed-Solomon codes, longitudinal redundancy control are considered. An analysis of the effectiveness of enhancing reliability by using Hamming code for data stored in the EAROM, showed that increasing the power of the coding alphabet leads to a decrease in the ratio of the number of rewritable control pages to the number of rewritable data pages, in turn, increasing the likelihood of overwriting data pages increases required number of control pages. Thus, Hamming codes that have a longer codeword length are more memory efficient. The final choice of the encoding algorithm depends on the performance of the MCPI, the degree of security of the stored data, and the degree of redundancy that is determined by the amount of memory.

References:

1. Wolfgang R., WolfgangE.Smart Card Hand book. WILEY, 2011. – 1025 стр.

2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. – 576 стр.

ВПЛИВ VR/AR ТЕХНОЛОГІЙ НА КІНЕМАТОГРАФ

Дегтярьов Євген Олександрович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

На тлі повсюдного ажіотажу навколо штучного інтелекту спостерігається зростання інтересу і до інших технологій, від яких чекають воістину революційних змін як в бізнесі, так і в повсякденному житті. Інтриги додають футурологи і коментатори, які змагаються в прогнозах, нагнітаючи захват і нервозність: «машини займуть більшу частину робочих місць», «доведеться вчитися і переучуватися все життя», «хто не вміє програмувати - не ввійде в світле майбутнє». Одна з цих технологій – віртуальна/доповнена реальність, яка починає розвивати значиму для нашого повсякденного життя галузь кінематографії.

«Майбутнє кіно» - саме так називають нетрадиційне кіно з використанням VR/AR технологій. Будь-який інвестор підтвердить: як би не був хороший продукт сам по собі, на нього потрібен попит. Сильна сторона VR / AR в тому, що глядач не дивиться на те, що відбувається з боку, а відчуває себе учасником дії. У кіновиробництва є в цьому відношенні козир: історії, всередині яких глядач неодмінно захоче побувати. Так, у 2017 році на Венеціанському кінофестивалі демонстрували вже кілька VR-проектів. Венеція вже відбудувала для показу таких робіт і організації супроводжуючих ці покази інсталяцій додатковий павільйон.

Перетворення традиційного фільму або серіалу в якийсь VR-формат, зрозуміло, не знищить кінематограф, проте перехід на новий носій потребують дотримуватися іншого набору правил. Простий переклад традиційних фільмів в формат 360 ° навряд чи може претендувати на успіх. У розробці імерсивних наративів (коли користувач може впливати на розвиток сюжету) потрібно орієнтуватися на два фактори користувацького досвіду: «втеча» і «емпатію». Це можливість опинитися в найнесподіваніших місцях і випробувати почуття співпереживання того, що відбувається. Найбільш очевидний підхід - дати користувачеві можливість відчути себе кимось іншим. Значні для успіху VR-оповідання чинники: рух і переміщення (глядач повинен мати можливість переміщатися по створеному для нього світу), звук (повинен бути функціональним - наприклад, підказувати, на що треба звернути увагу), місце розташування (місце, де відбуваються події, повинно бути сюжетно значущим).

Сценарії повинні враховувати бажання глядача самостійно вибирати, на що звертати увагу. Це значно обмежує диктат режисера і оператора і розширює інтерактивні можливості і права глядача. У візуальної частини це означає справжню революцію. До сих пір тільки автори вирішували, що показувати і як показувати. Тепер такі поняття, як ракурс, план, освітлення, глибина різкості, рух камери, переходи між сценами повинні кардинально змінитися. Рівно так само, як і співвідношення жанрів в телебаченні і кіно. Скажімо, документалістика і різного роду реаліті-шоу можуть отримати величезний імпульс до розвитку, а ось що буде з комедією і драмою, де дуже багато залежить від жорстко заданої драматургії, - велике питання.

VR-технології поки доступні не всім, але кіноіндустрія вже досягла неймовірних висот в суміжних областях. Один з найбільш вражаючих прикладів - інтерактивний фільм Netflix

«Чорне дзеркало: Брандашмиг», створений Чарлі Брукером і Аннабель Джонс. Під час перегляду глядачам періодично пропонують вибрати з двох можливих варіантів розвитку подій: чи повинен головний герой розповісти своєму психотерапевта про почуття до померлої матері чи ні, зізнатися вам йому, що ви дивитеся його по Netflix, і так далі.

За даними аналітиків з Goldman Sachs Internet Team, у телеканалу Netflix ще у 2017 році було 462 млн передплатників. Застосування технології віртуальної реальності не можна назвати масовим, але з часом ситуація кардинально зміниться. У довгостроковій перспективі віртуальна реальність здатна зайняти значну нішу в сфері розважального відео.

Проте, як і у випадку з відеоіграми, тут найскладніше сам процес створення контенту. Для зйомки фільмів за технологією віртуальної реальності необхідне використання спеціальних камер, які знімають кругові панорами на 360 градусів. Віртуальне присутність глядача повністю поміняє звичний підхід до написання сценарію і самого процесу зйомки фільму: через це буде складно спрогнозувати кількість коштів, які знадобляться знімальній команді. Одночасно з цим спроститься процес обробки матеріалу, завдяки панорамної зйомки операторам не потрібно буде працювати з безліччю камер. Але для початку продуктивної роботи кінокомпанії повинні виділити необхідні кошти для розвитку індустрії в віртуальної реальності.

За статистикою Goldman Sachs Internet Team, доходи Netflix в 2015 році склали $ 50 млрд. Використання технологій віртуальної реальності помітно розширить нинішній ринок онлайн-телебачення і кіно.

Висновок

Віртуальна реальність розвивається в наші дні досить швидко. За допомогою VR-шоломів і ігрових приставок кожен може, перебуваючи вдома, політати на винищувачі в Star Wars або на грифоні в World of Warcraft. Але до останнього часу було важко припустити, що технології VR стануть актуальними в глядацькому кіно. Поки що не зовсім зрозуміло, в яку гавань запливе корабель під назвою «VR-кіно». Зараз у нього рівні шанси стати справжнім мистецтвом і «продатися» масовій культурі. Тому VR-кіно може перетворитися з нішевої розваги в художню технологію, яка міняє світ на краще.

Література:

1. 9 сфер применения виртуальной реальности: размеры рынка и перспективы: https://vc.ru/flood/13837-vr-use

2. Как искусственный интеллект и виртуальная реальность меняют кино: https://www.vogue.ru/peopleparties/cinema/kak_iskusstvennyj_intellekt_i_virtualnaya_realnost_menyayut_kino

3. Как технологии виртуальной и дополненной реальности изменят индустрию развлечений: https://adindex.ru/publication/opinion/media/2018/07/9/172599.phtml

ЛІТАЮЧІ АВТОМОБІЛІ ТА ПАСАЖИРСЬКІ ДРОНИ

Дзицюк Андрій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В кінці 70-х – на початку 80-х років минулого століття, коли в поп-культурі та кіно почалась мода на наукову фантастику, літаючі автомобілі здавались чимось нереальним. Але час йшов, техніка не стояла на місці. І ось, в 2021-му році компанія General Motors представила футуристичну концепцію подібного апарату. І хоча на її реалізацію піде ще близько десяти років, вже зараз можна казати, що літаючі автомобілі – передвісник близького майбутнього.

На цьогорічній виставці CES фірма General Motors представила футуристичний концепт одномісного електричного безпілотника Cadillac eVTOL. Завдяки вертикальному зльоту і посадці цей самокерований автомобіль зможе переміщати пасажира над містом з даху на дах, приземляючись на спеціальні платформи. Він оснащений електричним мотором потужністю 90 кВт/год, який приводить в дію чотири ротора за допомогою акумуляторної батареї, що дозволяють електромобілю літати зі швидкістю до 90 км/год.

За запевненням General Motors, її літаючі таксі забезпечать пасажиру розкішне ізольоване подорож і панорамний вид на місто. Компанія також приступить до розробки двомісного безпілотника. Випускати незвичайний транспортний засіб планується під брендом Cadillac. Дрон розрахований для використання в мегаполісах в умовах складного трафіку. Літаючі «Кадилаки», за словами виробника, покликані забезпечити «нуль аварій, нуль викидів і нуль заторів», тобто звести до нуля ці три проблеми.

У свою чергу, для переміщення по землі General Motors придумав ще один прототип. Концепт Personal Autonomous Vehicle є повністю автономним мікроавтобусом без традиційних педалей і рульового управління. Незграбний дизайн машини нагадує літаючий дрон Vertical Take-Off and Landing Drone, а інтер'єр машини виконаний переважно у футуристичному стилі.

General Motors не єдина автомобільна компанія, яка веде роботи над літаючими транспортними засобами. На даний момент подібні розробки введе цілий ряд автовиробників. Так, компанія Hyundai має намір в 2028 році розпочати серійний випуск широкої лінійки літаючих автомобілів. Для цього

корейці вже створили окремий підрозділ. У свою чергу, концерн Fiat Chrysler Automobiles (FCA) заявив про намір випустити подібний транспортний засіб з можливістю вертикального зльоту і посадки. Також в проекті візьме участь компанія Archer з Каліфорнії.

Література:

1. https://mind.ua/ru/publications/20220850-ces-2021-10-vau-novinok-glavnoj-vystavki-elektroniki

2. https://inc-news.ru/auto/2:172096

3. https://www.autonews.ru/news/6000176c9a79473a5453da28

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ SMART CITY В УКРАЇНІ

Дзісяк Владислав Геннадійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Що таке Smart City?

Smart City (розумне місто) - це узагальнене поняття міської зони, що використовує різноманітні типи датчиків та електронних пристосувань для збору даних. Зібрані дані використовуються для управління комунальною власністю, ресурсами та використовуються для покращення сервісів міських служб та органів влади. Дані можуть бути отримані від жителів міста, різноманітних датчиків та пристроїв, що відповідно налаштовані для збору та обробки отриманих даних, керування та моніторингу систем водопостачання, електропостачання, газопостачання, міських електростанцій та станцій розподілу електроенергії, служби та системи збору/вивезення сміття. Загалом, подібно тому, як нервова система людини реагує на зміни в тілі, рішення та платформи технологічних гігантів, дозволяють побудувати систему керування містом, що буде працювати як нервова система цілого міста. Сучасні міста, в цілому, вже використовують певні інформаційні системи, для керування та розподілом ресурсів, проте концепція Smart City, передбачає певні ключові особливості.

Ключові особливості Smart City

Оскільки досить важко сформувати точне визначення концепції Smart City, через наявність різномаїття концепцій та визначень, виділяються чотири основні фактори, котрі здійснюють найбільший вплив:

1. Використання широкого спектра цифрових та електронних технологій в місті та суспільстві.
2. Використання ІКТ (інформаційно-комунікаційні системи) для трансформації життя та робочого середовища.
3. Впровадження цих технологій в державне управління.
4. Практика децентралізації, що об'єднує ІКТ та людей в автономні громади, котрі підвищують рівень інновації та наукових знань в суспільстві.

Передбачається, що Smart City використовує інформаційні технології та системи для:

1) Більш ефективного використання фізичної інфраструктури: будівництво, дороги, системи постачання комунальних послуг, на основі штучного інтелекту та автоматизованих систем керування та аналізу даних, для підтримки стабільно високого технологічного, культурного, та економічного зростання та розвитку міста.
2) Ефективної взаємодії з місцевими жителями по питанням місцевого самоврядування, та для прийняття рішень, прозорим шляхом на основі електронних систем, с ціллю підвищення залученості міських жителів у процеси планування та розвитку міста.
3) Місто та суспільство разом навчаються, пристосовуються, та впроваджують новітні системи керування та планування і тим самим оперативніше реагують на зміни та небезпечні виклики сучасності.
4) Використання смарт платформ та смарт-метрів, хмарних сервісів, безпровідних мереж з RFID чіпами- створюють революційні засоби збору, обробки та використання даних, що в подальшому використовуються для покращення та оптимізації роботи інфраструктури міста.

Успішна реалізація - запорука успіху

Одним із найуспішніших прикладів реалізації концепції Smart City є Шеньчжень. В цьому місті завдяки технологій розумного міста вдалося значно покращити роботу багатьох муніципальних сервісів. Наприклад, отримання підтвердження для безкоштовного навчання дітей, чи для мігрантів з інших країн в середньому займало 20 днів, після впровадження відповідних сервісів вдалося скоротити цей час до 2(!) днів, навіть, без необхідності відвідувати будь-які державні установи, достатньо лише 1 раз завантажити документи онлайн, та підтвердити свою особистість «офлайн». Також вдалося знизити рівень злочинності на 28%, а швидкість обробки та закриття однієї справи прискорити на 50%. Схожі показники зростання

ефективності роботи міських служб можливо спостерігати в будь-якому місті, що вдосконалилось до рівня «Smart City».

Розвиток в Україні

В Україні, на жаль, поки що концепція «розумного міста», в кращому разі, успішно реалізовується лише для отримання довідок, та безготівковому способу оплати проїзду в міському транспорті, а в гіршому навіть не реалізовуються, а лише призводить до чергових детективних історій вартістю в мільйони чи, навіть, мільярди гривень. Незважаючи на це більшість українських міст чудово підходять для реалізації концепції розумного міста, оскільки є такі фактори:

1. Відсутня необхідність зберігати існуючу інфраструктуру, оскільки, в більшості випадків, її необхідно створювати з нуля.
2. Необхідно скорочувати кількість державних посадовців для зменшення витрат та покращення швидкості надання послуг. Нестача кваліфікованих працівників повинна прискорити, а не сповільнювати цей процес.
3. Існуюча негативна криміногенна атмосфера в містах створює значні проблеми для жителів міста, погіршує безпеку, та призводить до появи тіньової економіки, зменшує інвестиційну привабливість міст.
4. Держана політика на децентралізацію влади дає можливість керівництву міст залишати в місцевому бюджеті більше коштів та самостійно визначати стратегію розвитку міста.

Проте, на жаль, існують також негативні фактори, що сповільнюють розвиток:

1) Низька зацікавленість органів місцевої влади у розвитку.
2) Страх перед новими технологіями у більшості місцевих жителів. Радіофобія як один із прикладів.
3) Низька ефективність існуючих органів влади та органів самоврядування.

Більшість із існуючих проблем легко вирішується правильною інформаційною політикою з боку місцевої влади, та ефективним управлінням з боку центральної влади. Місцевим жителям також слід контролювати місцеву владу, та самостійно об’єднуватися для вирішення проблем.

Література:

1. https://e.huawei.com/en/material/industry/smartcity/02ad4d5ab608492ea24659ec667f04bd

2. https://www.prostir.ua/?news=scho-take-smart-city-i-yak-vyhlyadaje-v-ukrajinskyh-realiyah

3. *https://tech.liga.net/technology/article/kak-glavnoe-prilojenie-stolitsy-kyiv-smart-city-stalo-kiiv-tsifroviy-pochti-detektiv*
4. *https://www.bbc.com/russian/features-50901826*

ТЕХНОЛОГІЯ ВИСОКОШВИДКІСНОГО БЕЗДРОТОВОГО ДОСТУПУ WI-FI 6 В СУЧАСНОМУ СВІТІ: ОСОБЛИВОСТІ БУДОВИ ТА ЗАСТОСУВАННЯ

Диняк Володимир Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У даній статті розглядається питання особливостей будови та застосування високошвидкісного бездротового доступу Wi-Fi 6 у сучасному світі.

Бездротовий доступ Wi-Fi 6 знаходить широке застосування в областях, де звичайні комп'ютери та дротову мережу не використовують. Наприклад, в новітніх офісах де люди працюють за мобільними пристроями, такими як планшети, ноутбуки та смартфони.

У статті розглянуться особливості будови бездротової мережі та застосування у різних галузях промисловості

Вступ

Інформаційні технології на сьогоднішній день розвиваються дуже стрімко, і кожного дня число електронних пристроїв збільшується в рази як вдома так і на роботі. А за останні роки дуже стрімкими темпами збільшується число мобільних пристроїв. Ці мобільні пристрої зазвичай потребують того, щоб їх підключили до мережі, постійно потрібен доступ в Інтернет і до загальних ресурсів локальної мережі.

Вирішити ці задачі можна за допомогою бездротових локальних мереж на базі стандарту Wi-Fi. В сучасному світі мережевих технологій, технологія бездротових мереж Wi-Fi є самою зручною в умовах мобільності, простоти установки і експлуатації. Wi-Fi (wireless fidelity – бездротова точність) - стандарт широкосмугового бездротового зв'язку із сімейства 802.11 який був розроблений в 1997р. Зазвичай, технологія Wi-Fi використовується для налаштування бездротових локальних комп'ютерних мереж, а також створення так званих гарячих точок високошвидкісного доступу до Інтернету.

Основна частина

Нове покоління, очікувано, збільшить швидкість Wi-Fi. Але, головне, Wi-Fi 6 (802.11ax) істотно спростить розгортання і експлуатацію бездротових мереж. Це важлива перевага, яке дозволить прискорити запуск Wi-Fi. Ключова особливість Wi-Fi 6 - здатність працювати в складному середовищі з перешкодами, включаючи міські умови з безліччю бездротових мереж. Новий

стандарт підтримує багатоантенні приймачі MU-MIMO, причому точка доступу обробляє трафік до восьми користувачів без втрати швидкості. У старих стандартах швидкість ділилася між користувачами, і звернення до клієнтських пристроїв велося по черзі, а не одночасно.

Таким чином, Wi-Fi 6 багаторазово збільшить пропускну здатність мереж і зможе ретранслювати трафік високошвидкісних мереж 5G. Більш того, Wi-Fi 6 використовує багатостанційний доступ з частотним поділом каналів (OFDMA). Ця технологія давно застосовується в мобільних мережах. У Wi-Fi 6 вона дозволить розділити канали для підключення десятків користувачів без катастрофічного падіння продуктивності мережі. В цілому, для Wi-Fi 6 знизяться затримки, виростуть ємність і швидкість мережі, покращиться енергоефективність і якість сигналу в складному середовищі.

Обмежений частотний ресурс. Частотний ресурс можна використовувати по-різному. Можна розділити його на максимально широкі відрізки, щоб забезпечити високу швидкість передачі даних при малій кількості пристроїв - і Wi-Fi 6 підтримує виділення каналів шириною до 160 МГц, - а можна виділити багато каналів мінімальної ширини, щоб працюючі на них пристрою не заважали один одному . І гнучкість, з якою здійснюється «перемикання» між цими підходами, визначає універсальність стандарту.

Поділ частот. У Wi-Fi 6 (по аналогії з мережами 4G) з'явилася підтримка OFDMA - множинного доступу з ортогональним частотним розділенням каналів. Щоб ефективніше використовувати спектр там, де на нього претендує багато користувачів, частотний канал розділяється на піднесучі шириною близько 78 кГц. Передача здійснюється на каналах, сформованих з деякої кількості піднесучих, кратного 26. По суті OFDMA - це використовувався раніше OFDM, оптимізований для безлічі користувачів мережі. OFDMA дозволяє поліпшити передачу даних в бездротовій мережі з високою щільністю пристроїв. Паралельно зменшується затримка доставки пакетів для кожного користувача окремо.

Більш високорівневе частотне планування можуть забезпечувати рішення від виробників обладнання. Так, Huawei інтегрує в своє залізо з підтримкою Wi-Fi 6 технологію DFA, яка забезпечує динамічне присвоєння частотних каналів - вибір неперекривающихся каналів в діапазоні 2,4 ГГц, перемикання в діапазон 5 ГГц (при наявності такої можливості) і т.д.

«Різнобарвний» спектр. Сьогодні не так багато бездротових мереж існують в ізоляції. А якщо поблизу є ще 5-10

точок доступу, значить їх зони обслуговування перекриваються, викликаючи ті самі конфлікти.

В основі Wi-Fi від початку було закладено механізм доступу до середовища передачі CSMA/CA з відправкою службових кадрів RST і CTS (запит на передачу - вільний для передачі). Якщо пристрою треба передати інформацію, воно слухає середу, і, коли та зайнята - чекає деякий час, щоб спробувати ще раз. Якщо ж середа вільна, воно відправляє запит на передачу (RST) і тільки після підтвердження (CTS) передає дані. Цей механізм донедавна не розбирав «свій - чужий»: хтось передає, значить треба мовчати і чекати своєї черги. Це викликало падіння швидкості передачі і збільшення часу очікування в мережах з великою кількістю пристроїв в безпосередній близькості один від одного.

Для вирішення цієї проблеми в Wi-Fi 6 закладений механізм «розфарбовування» (а точніше, маркування) пакетів в одних і тих же частотних каналах, які використовуються різними пристроями - BSS coloring - Basic Service Set Coloring. При такому розкладі, виявивши пакет з «чужим» кодом, пристрій проігнорує його. Допомогти процедурі повинно автоматичне регулювання порогів виявлення сигналу для «своїх» і «чужих», а також удосконалення механізму фокусування передачі в напрямку клієнтських пристроїв (про нього докладніше - далі).

До речі, час очікування в бездротових мережах регулюється механізмом NAV (Network allocation vector), який наказує станції «підглядати» в тривалість переданого кимось іншим пакета, щоб визначити, коли можна знову спробувати передати свій. І в Wi-Fi 6 з'явилося два окремих NAV: для пристроїв всередині «своєї» і «чужих» мереж. Нововведення дозволяє не «збивати» настройки чужими передачами і не помилятися з вибором часу для запиту передачі.

Поділ в просторі. Крім логічного маркування «свій-чужий» Wi-Fi може поділити клієнтів просторово. Пристрої попереднього стандарту вже «вміли» коригувати діаграму спрямованості передачі для декількох окремих користувачів (MU-MIMO). Фактично технологія дозволяє сформувати окремий промінь для користувача з пакетами, призначеними саме для нього. Однак в Wi-Fi 5 це працювало тільки на downlink. У Wi-Fi 6 той же механізм з'явився і на uplink, при цьому як і з downlink частотне планування здійснюється на стороні точки доступу. Одночасно було розширено кількість можливих підключень в два рази - до 8×8.

Очевидно, що технологія MU-MIMO 8 × 8 повинна підтримуватися пристроєм, а ефективність формування окремих просторових променів залежить від використовуваних виробниками рішень, зокрема, спрямованих антен. Наприклад, є розробка - Smart Antenna, що представляє собою антенну решітку, на якій для передачі або прийому з певного напряму в просторі вибирається задана конфігурація елементів (кожен елемент сам по собі може бути як всеспрямованим, так і вузько). В даному випадку антена - це вже не просто «залізяка», а поєднання апаратної частини і алгоритму вибору конфігурації. У кожної антени 16 режимів роботи, що для чотирьох антен (в одній смузі частот) дає 416 комбінацій. Алгоритм вибору між цими комбінаціями спрацьовує за часом при підключенні нового пристрою або при істотній зміні умов прийому раніше підключеним. Для переконфігурації відправляється кілька навчальних пакетів (з різних конфігурацій антен) - так вибирається нова оптимальна схема. Все це дозволяє забезпечити краще покриття бездротової мережі при наявності перешкод, в тому числі для переміщювання користувачів.

Застосування високошвидкісної бездротової мережі Wi-Fi 6 в сучасному світі.

«Сплячий» інтернет речей. Все більша частка пристроїв, підключених до бездротових мереж, так чи інакше відноситься до IoT. Тому в Wi-Fi 6 був закладений механізм, який дозволяє скоротити енергоспоживання пристроїв і зменшити кількість конкурентів за середовище передачі в кожен конкретний момент часу. Цей механізм отримав назву TWT (target wake time). Він має на увазі пробудження пристроїв інтернету речей по таймеру тільки тоді, коли потрібно зібрати дані. В інший час пристрій «спить» і не претендує на середу передачі.

В результаті нова версія стандарту дозволяє будувати мережі з більш високою ємністю, ніж Wi-Fi 5. Чотириразове зростання теоретичної ємності допоможе розгортанню мереж в місцях з високою щільністю споживачів - в громадських і навчальних зонах, ділових центрах, на об'єктах з великою щільністю датчиків інтернету речей . Поряд з цим Wi-Fi 6 залишається дуже гнучким - тобто з його допомогою можна організувати як доступ безлічі терміналів, так і бездротову мережу для передачі до кожного учасника, наприклад, 4K-відео з мінімальними затримками.

Роумінг – настройки від виробників. Обговорюючи мережі високої щільності, не можна не згадати роумінг при переміщенні клієнтських пристроїв між точками доступу. У стандарт закладені механізми, які дозволяють точкам не

заважати один одному, а також не "збивати з пантелику» сусідню підмережа, якщо пристрій нею не обслуговується. Але розподілом пристроїв між точками повинні займатися більш високорівневі системи - рішення від виробників заліза. Наприклад, пристрої Huawei підтримують балансування навантаження - рівномірний розподіл користувачів між точками доступу в зонах з великою щільністю мереж. При цьому для безперебійної передачі даних в момент перемикання клієнтського пристрою пакети для нього буферизуються і відправляються на нову точку.

Більшість описаних нововведень в мережах буде доступно тільки за умови їх підтримки клієнтськими пристроями. З урахуванням розвитку ринку і циклу життя пристроїв домінуючим на ринку Wi-Fi 6 повинен стати вже через рік.

Wi-Fi Mesh системи. Стандартні маршрутизатори виконують функції по елементарному принципу. Роутер підключений до мережі, а до самого роутера підключаються клієнти. Вони задіють маршрутизатор, щоб передавати дані між собою і мати доступ до Інтернет. У таких випадках швидкість буде визначена саме заданими пристрою технічними характеристиками. Також на якість впливатиме відстань, присутність тих чи інших перешкод і кількість підключених пристроїв. І завжди в будинку буде таке місце, де сигнал на стільки слабкий, що їм взагалі не можна скористатися, а то і взагалі пропадає. Це некомфортно.

Такі проблеми можна вирішити покупкою Wi-Fi репітерів, прокладкою окремого кабелю або використання додаткової точки доступу. Тільки ось кабель створює масу проблем. Їх присутність не естетично, прокладка вимагає ремонту. Точно так само і використання репітера не завжди допоможе. Адже репітером створюється окрема Wi-Fi мережу. До неї потрібно підключатися окремо вручну або чекати, коли пристрій сам зрозуміє, що це необхідно зробити. Та й швидкість від репітерів завжди нижче, ніж у основного маршрутизатора.

У комерційному сегменті проблеми такі ж, тільки більш масштабні. Тому багато хто використовує Mesh мережі. Чим же Mesh відрізняється від звичайного маршрутизатора? Вся справа в тому, що Mesh-мережа це не один пристрій, а кілька. Кожен окремий елемент відповідає за свою площу, де стежить за підключеними клієнтами і надає їм доступ до Internet. Що цікаво, так це те, що безпосередньо до Інтернет потрібно підключати тільки головний модуль (базу). Решта модулі підключаються до головного модулю для отримання доступу і роздачі його приєднаним клієнтам. Wi-Fi мережу в такому

випадку створюється єдина для всієї сумарної площі від всіх модулів.

В Mesh-мережах аналізується кожен зв'язок між модулями. Самі модулі обмінюються даними про всіх підключених клієнтів. І саме мережа вирішує, до якого модулю підключити клієнта, щоб у нього був найкращий сигнал. До того ж передача даних між гаджетами всередині мережі може відбуватися і без участі головного модуля. Висока швидкість доступу до Internet зберігається за рахунок того, що в Mesh-рішеннях присутній окремий канал для обміну інформацією між собою, тому інформація направляється по найбільш короткому шляху. Як бачите, можна порівняти з тим, що Mesh-мережі складаються з пов'язаних між собою маршрутизаторів.

Використання в різних громадських місцях, підприємствах та приватних помешканнях. Технологію високошвидкісного бездротового доступу використовують в усьому світі. Наприклад всім відомо як люди жаліються на погано працюючий Wi-Fi в місцях масового скупчення людей та в громадських місцях таких як аеропорти, стадіони, парки, торгівельні центри, офіси і тд. Перехід на Wi-Fi 6 вирішить всі проблеми з доступом в інтернет в таких місцях.

Висновки

У даній статті було розглянуто особливості будови та застосування технології високошвидкісного бездротового доступу Wi-Fi 6 у сучасному світі. Досліджено основні характеристики бездротового доступу Wi-Fi 6, а також області їх використання.

В статті наведено декілька прикладів використання технології високошвидкісного бездротового доступу Wi-Fi 6, але якщо подивитись глибше то можна зрозуміти що дану технологію можуть використовувати абсолютно в усьому світі, від власних будинків та маленьких підприємств, до найбільших у світі заводів чи офісів, також якщо подивитись на повний перехід з кабельних технологій на бездротовий то це позитивно вплине та навколишнє середовище, адже не буде потрібно прокладати тисячі кілометрів мідного кабелю в кожний куточок землі.

Література:

1. Группа стандартов WiFi IEEE 802.11 [Електронний ресурс] – Режим доступу до ресурсу: http://wi-life.ru/texnologii/wi-fi/wi-fi-standarty

2. WiFi6 [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/article/449116/

3. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2019. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2

4. Азаров О. Д. Комп'ютерні мережі: навчальний посібник / О. Д. Азаров, С. М. Захарченко, О. В. Кадук. – Вінниця : Вінницький Національний Технічний Університет, 2013. – 371 с. - ISBN 978-966-641-543-4

ОСНОВНІ ПОНЯТТЯ GRID LAYOUT

Долинна Ельвіра Русланівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

CSS Grid Layout спроектований таким чином, щоб працювати разом з іншими частинами CSS і складати з ними закінчену систему створення макетів сторінок.

1. Постановка задачі. Ознайомити слухачів з технологією Grid Layout.

2. Мета дослідження. Дослідити, що таке Grid Layout та для чого вони призначення та в чому його переваги.

3. Результати дослідження. Grid являє собою перетинається набір горизонтальних і вертикальних ліній - один набір визначає стовпці, а інший рядки. Елементи можуть бути поміщені в сітку, відповідно рядках і стовпцях. Grid має наступні функції:

- фіксовані і гнучкі розміри смуг;
- розташування елемента;
- створення додаткових смуг для зберігання контенту;
- управління вирівнюванням;
- управління перекриваються контентом.

Призначення Grid Layout - повністю змінити спосіб проектування призначених для користувача інтерфейсів, дизайн яких заснований на сітці. Так, за допомогою CSS завжди можна було створити макет, але кожен підхід має свої недоліки і, по суті, є хаком. Спочатку для верстки використовувалися таблиці, потім float, позиціонування і inline-block ... Дані інструменти не були розроблені спеціально для створення колоночного макетів, і багато необхідні функції були недоступні (наприклад, вертикальне центрування). Рішення практично кожної проблеми прирівнювалося до «танцю з бубном».

Модуль Flexbox частково полегшив завдання веб-розробникам, але все ж він більше підходить для створення простих одновимірних макетів, а не складних двовимірних (до речі, Flexbox і Grid відмінно працюють в парі). Grid - це перший CSS-модуль, створений спеціально для розробки повноцінних макетів і усунення проблем, які ми довгий час вирішували обхідними шляхами.

Основна відмінність між CSS Grid Layout і CSS Flexbox Layout в тому, що flexbox призначений для позиціонування елементів в одному напрямку, тобто, або в рядку, або в колонці. Grid же був розроблений для позиціонування елементів в двовимірної системі, тобто, для одночасного позиціонування і в рядку, і в колонці. Однак, в двох специфікаціях є деякі спільні риси, і якщо ви вже навчилися приборкувати flexbox, ви побачите подібності, які допоможуть вам розібратися і з Grid.

4. Висновки та перспективи.

CSS Grid Layout - це найпотужніший інструмент для створення розмітки, який доступний в CSS на сьогоднішній день. Це двовимірна система, яка може містити рядки і стовпці (на відміну від модуля Flexbox, який в цілому є одновимірної системою).

Література:

1. *https://idg.net.ua/blog/uchebnik-css/razmetka-css/grid*
2. *https://developer.mozilla.org/ru/docs/Web/CSS/CSS_Grid_Layout/Basic_Concepts_of_Grid_Layout*
3. *https://developer.mozilla.org/ru/docs/Web/CSS/CSS_Grid_Layout/Relationship_of_Grid_Layout*

ОСНОВНІ ПОНЯТТЯ REACT

Долинна Ельвіра Русланівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Інструмент JavaScript з відкритим вихідним кодом.

1. Постановка задачі. Ознайомити слухачів з технологією React.

2. Мета дослідження. Дослідити, що таке React та для чого вони призначення та в чому його переваги.

3. Результати дослідження. React - найпопулярніша бібліотека JavaScript для розробки користувальницького інтерфейсу (UI). React пропонує відмінний відповідь на вхідні дані користувача, використовуючи новий метод візуалізації веб-сайтів. Компоненти цього інструменту були розроблені Facebook. Він був запущений як інструмент JavaScript з відкритим вихідним кодом в 2013 році. В даний час React випереджає своїх основних конкурентів, таких як Angular і Bootstrap, дві найбільш продаються бібліотеки JavaScript свого часу.

Ось деякі з причин, щоб використовувати його:

1) Простота в використанні:

React - це JavaScript бібліотека GUI (англ) з відкритим вихідним кодом, зосереджена на одній конкретної мети -

ефективному виконання завдань в рамках розробки призначеного для користувача інтерфейсу. Його можна віднести до категорії "V" в архітектурному шаблоні MVC (модель-вид-контролер).

2) Підтримує Java-компонент багатократного використання:

React дозволяє повторно використовувати компоненти, які були розроблені в інших додатках, що використовують ту ж функцію. Можливість повторного використання компонента є явною перевагою для розробників.

3) Просте написання компонентів:

Компонент React створити простіше, оскільки він використовує JSX (англ), опциональное розширення синтаксису JavaScript, яке дозволяє комбінувати HTML з JavaScript. JSX - це відмінна суміш JavaScript і HTML (англ). Воно робить весь процес написання структури сайту зрозумілішим. Крім того, розширення також значно спрощує рендеринг декількох функцій. Хоча JSX може бути не найпопулярнішим розширенням синтаксису, воно довело свою ефективність при розробці спеціальних компонентів або додатків великого обсягу.

4) Краща продуктивність з Virtual DOM:

React ефективно оновлює процес DOM (об'єктна модель документа). Можливо, ви вже й самі знаєте, що цей процес може викликати багато розчарувань під час розробки веб-додатків. На щастя, React використовує віртуальні DOM, тому ви можете уникнути багатьох проблем.

5) SEO friendly:

React дозволяє створювати призначені для користувача інтерфейси, до яких можна отримати доступ з різних пошукових систем. Ця особливість є величезною перевагою, тому що не всі JavaScript-фреймворки оптимізовані під SEO (англ).

4. Висновки та перспективи.

React - найпопулярніша бібліотека JavaScript для розробки користувальницького інтерфейсу (UI). React пропонує відмінний відповідь на вхідні дані користувача, використовуючи новий метод візуалізації веб-сайтів.

Література:

1. *https://www.hostinger.com.ua/rukovodstva/chto-takoe-react/*
2. *https://ru.reactjs.org/tutorial/tutorial.html*
3. *https://ru.wikipedia.org/wiki/React*

ПЕРСПЕКТИВИ РОЗВИТКУ VR

Дремлюк Богдан Леонідович

Державний університет телекомунікацій

Що таке віртуальна реальність?

Віртуальна реальність (VR) - це комп'ютерне середовище, де сцени та об'єкти здаються справжніми, завдяки чому користувач відчуває, що штучно створений навколо нього світ - справжній. Це середовище сприймається через пристрій, відомий як гарнітура або шолом віртуальної реальності. VR дозволяє нам зануритися у відеоігри так, ніби ми є одним із персонажів, навчитися робити операції на серці або покращити якість спортивних тренувань, щоб максимізувати продуктивність.

Хоча це може здатися надзвичайно футуристичним, його походження не настільки нове, як ми могли б подумати. Насправді багато людей вважають, що одним із перших пристроїв віртуальної реальності називали Sensorama, машину із вбудованим сидінням, яка відтворювала 3D-фільми, видавала запахи та генерувала вібрації, щоб зробити досвід максимально яскравим. Винахід датується серединою 1950-х років. Подальші технологічні та програмні розробки протягом наступних років спричинили за собою поступовий розвиток як у пристроях, так і в дизайні інтерфейсу.

Відмінності з доповненою реальністю

Незважаючи на те, що це технологія, яка виникла десятки років тому, багато людей досі не знайомі з концепцією віртуальної реальності. Також досить часто плутають термін Віртуальна реальність із доповненою реальністю.

Головна відмінність між ними полягає в тому, що віртуальна реальність будує світ, в який ми занурюємось, завдяки певній гарнітурі. Він повністю заглиблюється, і все, що ми бачимо, є частиною навколишнього середовища, штучно сконструйованого за допомогою образів, звуків тощо. З іншого боку, в доповненій реальності (AR) наш власний світ стає рамкою, в яку поміщаються предмети, зображення або інші подібні речі. Все, що ми бачимо, знаходиться в реальному середовищі, і, можливо, не буде категорично необхідним постійно носити з собою гарнітуру. Найяскравіший і найбільш поширений приклад цієї концепції - Pokémon Go.

Однак існує також поєднання обох реальностей, яке називається змішаною реальністю. Ця гібридна технологія дозволяє, наприклад, бачити віртуальні об'єкти в реальному світі та створювати досвід, в якому фізичне та цифрове практично неможливо розрізнити.

Основні застосування віртуальної реальності

Цього досить щодо теорії, яка проектує нас у майбутнє. У яких секторах фактично використовується віртуальна реальність сьогодні? Медицина, культура, освіта та архітектура - це деякі сфери, які вже скористались цією технологією. Від відвідування музею до розтинання людського тіла, VR дозволяє нам переходити межі, які в іншому випадку були б немислимі.

Майбутнє віртуальної реальності

Віртуальна реальність - одна з технологій з найбільшим прогнозованим потенціалом для зростання. Згідно з останніми прогнозами IDC Research (2018), інвестиції у VR та AR збільшаться у 21 разів протягом наступних чотирьох років, досягнувши 15,5 млрд євро до 2022 р. Крім того, обидві технології стануть ключовими для планів компаній щодо цифрової трансформації та їх витрати в цій галузі перевищать витрати на споживчий сектор до 2019 року. Тому очікується, що до 2020 року більше половини великих європейських компаній матимуть стратегію VR і RA.

Сьогодні ринок вимагає додатків, які виходять за рамки відпочинку, туризму чи маркетингу та є більш доступними для користувачів. Віртуальні інтерфейси також потрібно вдосконалити, щоб уникнути таких дефектів, як відсікання, через яке певні тверді об'єкти здаються такими, ніби їх можна пропустити. Або звести до мінімуму наслідки, які виробляє ВР у людей, серед них хвороба руху, яка складається із запаморочення, спричиненого невідповідністю руху нашого тіла до того, що спостерігається у віртуальному світі.

Великі технологічні компанії вже працюють над розробкою гарнітур, які не потребують кабелів, і які дозволяють бачити зображення в HD. Вони розробляють гарнітури віртуальної реальності у форматі 8K та мають набагато потужніші процесори. Навіть говорять, що в найближчі кілька років вони можуть інтегрувати штучний інтелект. Останній стандарт 5G також може надати дуже цікаві сценарії розвитку VR. Цей стандарт дозволить підключати більше пристроїв та великі спільноти користувачів. Крім того, його майже непомітна затримка дозволить споживачам отримувати зображення в режимі реального часу майже так, ніби вони бачать їх на власні очі.

Все це означає, що «Віртуальна реальність» вже не є науковою фантастикою. Він інтегрований у наше сьогодення, і в найближчі роки це призведе до прогресу, який сформує майбутнє.

Література:

1. *Augmented: Life in the Smart Lane by Brett King*

2. *https://vrmotion.com.ua/ru*
3. *https://dailytechinfo.org/infotech/110-icube-texnologiya-sozdaniya-trexmernoj-virtualnoj.html*

ВИКОРИСТАННЯ 5G В МЕДЕЦИНІ

Дремлюк Богдан Леонідович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Незважаючи на інтенсивні зусилля, все ще існують величезні проблеми, з якими доводиться стикатися, забезпечуючи послуги охорони здоров’я для швидкозростаючого та старіючого населення. Останні спостереження викликали занепокоєння з приводу високих витрат на охорону здоров'я, дисбалансу медичних ресурсів, неефективне адміністрування системи охорони здоров'я та незручності в медичному досвіді. Шлях до подолання цих викликів полягає у всебічному використанні передових технологій, зокрема IoT, big data, AI та 5G для покращення якості медичних послуг, і тим часом скорочення загальних витрат на охорону здоров'я. Заглибимося у справи, які зосереджуються на застосуванні технології бездротової передачі 5G в охороні здоров'я.

Термін "5G" відноситься до п'ятого покоління технології бездротової передачі, яка буде вироблятися епохальний вплив на багато аспектів сучасного суспільства, особливо в галузі охорони здоров'я. Хоча технологія 5G керується власним набором параметрів, однак деякі унікальні особливості найбільше цінуються в галузі охорони здоров’я, такі як: швидкість передачі даних, наднизька латентність (затримка), висока пропускна здатність. Що стосується швидкості передачі, 5G буде пропонувати швидкість передачі даних до 10 Гбіт / с, а саме від 10 до 100 разів покращення порівняно з 4G та 4G LTE. Крім покращення швидкості, ще однією відмінною рисою 5G є низька затримка. Насправді латентність менше однієї мілісекунди (мс) в еру 5G, майже еквівалентна нульовій реакції даних час у реальному світі. Крім того очікується, що 5G розкриє величезний потенціал IoT.

Що означає 5G для охорони здоров’я - це питання, над яким варто задуматись. Хоча 5G для більшості людей означає швидший Інтернет. Вона також значно сприятиме інтеграції VR та AR, що є критично важливим для всебічного навчання з реабілітації, а також реабілітації кінцівок та телемедицини завдяки своїм технічним характеристикам. Тісно пов’язана із

застосуванням VR та AR в охороні здоров'я вправа на реабілітацію кінцівок, включаючи роботизовану підтримку дрібної моторики кінцівок, компенсацію сили тяжіння, індивідуально підібрану програму відеотренінгу. Застосування VR в охороні здоров'я не є новою технологією, що з'явилася в епоху 5G, натомість медично застосовну технологію можна простежити щонайменше двадцять років тому, але вона не була повністю готова, до зрілості 5G.

Важливим обмеженням в сучасних мережах передачі данних є затримка. Життєво важливі сигнали можуть передаватися на медичне обладнання або монітори екрану в лікарні з майже нульовою затримкою якщо з'явиться можливість використовувати мережі п'ятого покоління, під час інтуїтивного хірургічного навчання або навіть при дистанційній хірургії. Очевидно, що поточний 4G не справляється з такими задачами. Важливішим моментом є те, що 5G є досить потужним, щоб одночасно підтримувати тисячі медичних пристроїв, починаючи від датчиків і закінчуючи мобільними телефонами, медичним обладнанням, відеокамерами та доповнюючи 4k або навіть 8K телевізором ультрависокої чіткості чи низки систем моніторингу.

Мережа 5G робить можливими певні процедури при менших витратах. Так зробивши наприклад біопсію, данні аналізу можна миттєво переслати в різні корпуси мед університету. Як один із варіантів, в клініках можливе встановлення так званих розумних центрів. Які будуть контролювати розклад лікарів та пацієнтів, слідкувати чи зайнятий кабінет, або де саме зараз проводять операцію. Що в свою чергу зменшить очікування і паперову тяганину. Медицина відстає від інших областей за кілька років. Однак використання 5G та доповненої реальності стимулюватиме зміни у секторі здорового харчування та прискорення інновацій. Найкращий вплив 5G на навчання та професійне навчання лікарів. У той час, коли лекція студентів-медиків може отримати інформацію лише на 10%, нові технології можуть розширити їх досвід та допомогти отримати більше знань. Наприклад, лікар з практичними навичками може навчати інших віддалено завдяки швидкості телекомунікацій.

Як приклад можна привести досвід із Росії. У технопарку «Сколково» в пілотній зоні 5G новатори Білайн та Huawei спільно з лікарями GMS Hospital об'єдналися для проведення хірургічної операції. Операція проводилася при співпраці віддалених медичних експертів. Обмін необхідною інформацією між операційним хірургом та спеціалістами-консультантами

здійснюється через відео-конференц-зв'язок 4K. Обговорення включає історію хвороби пацієнта, а також консультації та інструкції експертів у режимі реального часу. У результаті у пацієнта було успішно видалена ракова пухлину. Лапароскопія (огляд черевної порожнини і таза) і камера 4K були підключені до мережі 5G. Також у процесі використовувалась консоль для анестезіології, додаткові камери та мультимедійна біла дошка.

Однак не варто очікувати, що «розумні» машини швидкої допомоги заполонять все місто. Справа не в складності технології – лікарі відмічають, що за порівнянням з деяким більшим обладнанням, гарнітура VR не особливо дорога чи складна у використанні. Потрібно переконатися, що нові інструменти повністю безпечні для пацієнта. Медицина не може простити собі технічні помилки чи якийсь збій, тому система екстреної телемедицини повинна бути абсолютно надійною та безпечною.

Література:

1. *Wearable Systems and Antennas Technologies for 5G, IOT and Medical Systems By Albert Sabban*
2. *https://www.rcrwireless.com/20200204/5g/4-ways-5g-is-transforming-medical-field*
3. *https://www.ericsson.com/en/reports-and-papers/5g-healthcare*

ЕКЗОСКЕЛЕТ GUARDIAN XO

Дудник В'ячеслав Романович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В повсякденному житті нам регулярно доводиться стикатись із важкою фізичною працею. Комусь рідше, комусь частіше. Але інколи ми просто не в змозі підняти ту чи іншу річ через її надмірну вагу. Для таких випадків, а також для ряду інших, американська компанія Sarcos Robotics розробила екзоскелет Guardian XO.

Sarcos Robotics не перший рік займається розробкою комерційно доступного повнорозмірного екзоскелета для подібних умов. Тепер компанія показала фінальну версію пристрою. Щоб почати працювати з екзоскелетом, людина заходить всередину конструкції і надійно прикріплюється до неї за допомогою ременів і жилета. Після цього робот, по суті, дублює дії людини, зчитуючи його рухи і зусилля, і повторюючи їх з урахуванням пропорцій: розробники відзначають, що співвідношення зусиль, що прикладає людина, та зусиль робота становить до одного до 20.

Людина може поміняти насадки на кінцях рук, залежно від завдань. Час роботи екзоскелету – близько двох годин. Якщо

акумулятор розрядився, його можна швидко поміняти, не розбираючи пристрій. Робот складається з безлічі секцій, що приводяться в рух за допомогою електромоторів. Їх робота обмежена як програмно, так і механічно. Наприклад, якщо робот з якоїсь причини втратить електроживлення, руки плавно опустяться, а не різко впадуть. Крім того, ширше, ніж дозволяє людське тіло, екзоскелет не може розвести руки. Це забезпечує додаткову безпеку.

Доступні сьогодні серійні моделі екзоскелетів заточені під конкретну виконувану задачу і, як правило, підсилюють тільки конкретну частину тіла - як, наприклад, екзоскелет для ніг від LG. Це дозволяє будувати більш легкі та ефективні пристрої, але такі екзоскелети не підходять для вирішення інших завдань і мало схожі на повнорозмірні роботизовані костюми з наукової фантастики, на кшталт костюму Залізної людини з кінематографічного всесвіту Marvel.

Довгий час прототипи були на гідравліці і вимагали кваліфікованого оператора для управління, але з розвитком робототехніки з'явилася можливість перейти на електроприводи і компанія на початку 2019 року оголосила, що працює над створенням першого серійного повнорозмірного екзоскелету. Для управління їм не потрібно буде володіти специфічними навичками. В кінці 2019 року Sarcos представила модель, яка отримала назву Guardian XO. Екзоскелет може піднімати вантаж до 90 кілограм, при цьому оператор буде відчувати навантаження на рівні 4,5 кілограм.

На початку 2020 року компанія запустила пілотний проект з авіакомпанією Delta Air Lines, в рамках якого екзоскелети застосовуються для завантаження багажу, а тепер Sarcos показала і інші можливі сценарії застосування Guardian XO. В опублікованому ролику екзоскелет використовується не тільки для навантаження сумок і ящиків на стрічку транспортера і стелажі, але виконує і інші завдання - наприклад, допомагає штовхати візок з важким вантажем і змонтувати колесо.

Для переміщення вантажів використовуються різні насадки на роборукою. Так, для валіз і важких ящиків з мотузковими ручками використовуються довгі гаки, а для перекладання покришок - насадка з двома загнутими вниз пластинами. У ролику, який представила компанія Sarcos Robotics, показано також, що оператор може легко відпустити рукоятку управління роборукою і зробити якісь дрібні рухи сам.

Література:

1. *https://nplus1.ru/news/2020/03/07/lend-a-robohand*
2. *https://nplus1.ru/news/2019/12/11/sarcos*

3. https://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Guardian_XO_(%D1%8D%D0%BA%D0%B7%D0%BE%D1%81%D0%BA%D0%B5%D0%BB%D0%B5%D1%82)

BRAIN NAVI: РОБОТ ДЛЯ ВЗЯТТЯ МАЗКІВ З НОСА

Дудник В'ячеслав Романович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Минулий 2020-й рік змінив наше сьогодення, змусивши поглянути на світ інакше. З'явившись несподівано й нізвідки, коронавірус COVID-19 ускладнив наше життя та поставив багато питань ы проблем як перед звичайними людьми, так і перед науковцями. В ході пошуку відповідей та рішень, тайванська фірма Brain Navi розробила робота, який покликаний спростити тестування пацієнтів, хворих на COVID-19.

Пандемія стала причиною масового тестування на предмет зараження вірусом SARS-CoV-2. Процедура взяття носового мазка може бути небезпечною як для медика, що її виконує, так і для близької людини, яка інструктує пацієнта, як це зробити. Для вирішення цієї проблеми розроблений робот, який здатний виконувати цю процедуру самостійно. Він може дозволити запобігти можливому розповсюдженню вірусу на місці тестування та розширити тестування на вірус, що викликає COVID-19.

Роботизований пристрій під назвою Nasal Swab Robot був презентований на виставці Bio Asia Taiwan 2020. В пристрої використовуються функції навігаційної системи роботизованої хірургії головного мозку, а також розпізнавання обличчя та тривимірні зображення.

Пацієнту прикріплюють особливий зажим на ніс, аби апарат міг знайти певні точки. Також йому надягають на голову металеву скобу, щоб голова не смикалася при заборі мазка і залишалася рівною. Робот вводить в ніс довгий шпатель для взяття мазка. Пізніше він поміщається у спеціальний закритий контейнер. Пристрій може перевіряти пацієнтів на 10 хвилин швидше за людей. Людині потрібно в середньому 15 хвилин, роботу - всього 5 (взяття мазка триває 10 секунд). Наразі його ще побоюються, надаючи перевагу "живим" контактам.

Новий пристрій заснований на деяких фундаментальних функціях робота NaoTrac тієї ж компанії, який призначений для нейрохірургічної навігації і вже використовувався в більш, ніж десяти операціях в тайванському медичному центрі Хуалянь Цзи-Чі.

Nasal Swab Robot ніде поки не отримав офіційного схвалення на використання від галузі охорони здоров'я, але

відзначається, що компанія-розробник отримала дозвіл на клінічні випробування в Тайвані та чекає на дозвіл від FDA на екстрене використання цього пристрою в США.

Література:

1. https://maximum.fm/inzheneri-stvorili-robota-yakij-testuvatime-lyudej-na-covid-19_n183038

2. https://evercare.ru/news/v-tayvane-razrabotan-robot-dlya-vzyatiya-mazkov-iz-nosa-dlya-testirovaniya-na-covid-19

3. https://zdrav.expert/

ПЕРЕВАГИ ТА НЕДОЛІКИ ВВЕДЕННЯ В ЕКСПЛУАТАЦІЮ ЕЛЕКТРОННОГО ОБЛІКУ МАЙНА

Євдоченко Степан Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Дослідження присвячено модернізації малого та середнього бізнесу задля підвищення продуктивності роботи окремих відділів (відділу керування, системних адміністраторів) за рахунок доступності та простоті отримання необхідних даних. Аналіз існуючого представника сфери IT (ТОВ «ОЛГА») показав, що не зважаючи на можливі затрати та незручності на початку налаштування мережі в подальшому це обов'язково принесе результати.

На даний момент інформаційні технології продовжуючи розширяти спектр програмного забезпечення збільшують його вибір під певні конкретні задачі, як от визначення середовища та бази даних під наші цілі. Складність в налаштуванні може грати ключову роль для великого бізнесу, який може дозволити собі власний відділ програмістів та навіть власне програмне забезпечення. Однак малий бізнес не зможе витримати таких затрат. Саме тому ми й звернемось до спеціалізованих програм.

Пропонується використовувати для збереження даних повноцінне програмне забезпечення «1С:Підприємсво 8» яке дозволяє аналізувати, зберігати та моніторити діяльність відразу декількох підприємств або відділів [1][2]. Окрім цього необхідно щоб наше програмне забезпечення дозволяло:

- фільтрувати по типу, категорії, ціні і стану майнову базу.
- вираховувати актуальні звіти по наявним змінам в обліку за певний період та за час всього існування об'єкта/філії/відділу.
- проводити оцінку рентабельності підприємства з визначенням слабких ланок кожної філії.
- зберігати в доступі дані про відповідальних осіб кожного об'єкта/філії/відділу.

- проводити списання та інвентаризації майна з видачею унікальних номерів кожному об’єкту з кожної категорії.

- створювати, контролювати, закривати і передавати заявки між будь-якими працівниками підприємства.

- реєструвати працівників та контролювати початок робочого дня через вхід в базу.

Головними вимогами будуть:

- Гнучкість програмного забезпечення для внесення змін в майбутньому.
- Помірні ціни на використання і підтримку ліцензованого програмного забезпечення.
- Надійність та стабільність роботи.
- Низьке навантаження на апаратну частину.
- Доступність для кожного користувача тільки актуальної для нього частини

Врахування зазначених показників дозволяє забезпечити використання єдиного рішення у вирішенні широкої варіації завдань, оптимізуючи робочий процес в необхідній мірі.

Література:

1. «Самоучитель системного администратора 5-е издание» Д. Колесниченко, А. Кенин.

2. «1С:Предприятие 8.1». М. Радченко

СУЧАСНІ САЙТИ ЯК ПРОГРЕСИВНІ ВЕБ-ДОДАТКИ

Єрещенко Олена Дмитрівна

Харківський Національний Університет ім. Семена Кузнеця

м. Харків

PWA або прогресивний веб-додаток (англ. progressive web application) – це технологія, яка додає сайту функціональність додатку. Бути додатком не означає, що PWA тільки для мобільних пристроїв. Вони також можуть бути встановлені на настільних комп’ютерах або ноутбуці. Можливо, що багато хто користувався такими додатками раніше, але навіть не зрозумівши цього. При відвідуванні деяких сайтів надходить пропозиція додати його на головний екран. Якщо її прийняти, значок сайту миттєво з’явиться серед ваших інших додатків.

Важливий момент – PWA встановлюється на пристрій користувача в два кліка. Це відбувається в обхід Play Маркет, а також забороні встановлювати додатки з невідомих джерел. Антивірусна програма також не забороняє дану дію. Розглянемо переваги використання PWA в сучасних проєктах.

Швидкість. Завантажується швидше, ніж звичайні сайти, завдяки технології Service Workers. Вона дозволяє швидко завантажити сайт вперше та ще швидше при подальших діях, оскільки відбувається кешування всього вмісту і відображення його при необхідності.

Розмір. У порівнянні з нативними додатками, PWA значно менші та іноді навіть менше 1 Мб, тоді як середній розмір додатку IOS становить 38 Мб, Android на 60% менший - 15 Мб [2].

Режим офлайн. Доступність в режимі офлайн також можлива завдяки технології Service Workers. При належній інтеграції технології весь вміст попередньо завантажується під час першого відвідування PWA та відображається після цього за допомогою Javascript, завдяки чому PWA є новим підходом при створенні сайтів, робота в офлайні для яких є необхідною.

Безпечність. Працює по захищеному протоколу HTTPS.

Кросплатформність. PWA, що був створенний, дає можливість отримати доступ через будь-які мобільні платформи, такі як Android, IOS, Windows, Linux, тощо, оскільки PWA – це браузер.

Оновлення. Оскільки непотрібно завантажувати PWA з сторонніх магазинів, таких як Apple Store, Google Play, Microsoft Store, тому оновлення додатку відбувається звичайним оновленням сайту [1].

Індексація. PWA технічно все ще є сайтом, його вміст може бути проіндексовано та відкрите для пошукових систем, таких як Google, Yandex тощо. Це відкриває можливості для SEO (оптимізація пошукових систем), що дозволяє PWA досягти більшої кількості користувачів порівняно з нативним додатком.

Публікація. З нативними додатками процес публікації іноді може бути справжнім «болем». Подавши свою програму в магазини додатків, з нетерпінням чекаючи декілька днів, можна отримати відмову з тієї причини, яка потребує виконати деякі невеликі кроки. А в деяких випадках програма взагалі ніколи не буде прийнята. Це стало актуально в деяких випадках, наприклад, для Huawei та їх конфліктом з Google, який залишив телефони Huawei без Google сервісів, а також користувачів, які не бажають користуватися Google сервісами взагалі. Тому в подальшому кількість користувачів додатком PWA буде збільшуватись.

Вартість розробки. Оскільки PWA розробляється один раз, а потім доступне для будь-яких мобільних платформ і браузерів, які її підтримують, вартість розробки для PWA невелика в порівнянні з нативними додатками. Ще одна причина полягає в тому, що PWA використовує мови програмування та технології, які більш зрозумілі і мають значно більшу базу розробників.

Обмеження. Поки не виявлено. Обмеження можуть бути тільки в функціоналі, але це залежить не від самого додатка, а від функціоналу який в нього закладено.

Важливо, що майже всі сучасні браузери підтримують PWA (наприклад Chrome, Firefox, Opera, браузер Android, браузер Samsung тощо), але ще залишаються деякі браузери, які відмовляються підтримувати PWA, наприклад Safari[4]. Це пов'язано з тим, що підтримка додатку PWA означатиме підтримку їх у майбутньому, а це, для компаній, таких як Apple, яка орієнтована на нативні додатки, не вигідно. Як показала практика, що впровадження PWA дає значні результати. Ось декілька прикладів: Tinder, завдяки технології, скоротив час завантаження сторінок з 11,9 до 4,69 секунди; PWA Tinder на 90% "легше", ніж їх нативний додаток (PWA Uber майже нічого не важить і завантажується за 3 секунди навіть в мережах 2G); OLX завдяки PWA підвищив CTR оголошень майже у 1.5 рази та зменшив кількість відмов на 80%.

Література:

1. Українські сервіси Інтернет-моніторингу. URL: https://ain.ua/2010/03/19/ukrainskie-servisyinternetmonitoringa. (дата звернення 01.02.2021).

2. Uptrends: Website Monitoring and Web Performance Monitoring. URL: https://www.uptrends.com. (дата звернення 28.01.2021).

3. Progressive Web. URL: https://codelabs.developers.google.com/codelabs/your-first-pwappru/index.html?index=..%2F..%2Flangru#0.(дата звернення 10.02.2021).

4. Progressive Web Apps. URL: https://developers.google.com/web/progressive-web-apps/. (дата звернення 08.02.2021).

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Заєць Марія Вікторівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Результати наукових досліджень показують, що інформація і наукові знання останніми роками грають все більшу роль в житті суспільства. Про інформацію сьогодні говорять як про стратегічний ресурс суспільства, що визначає рівень розвитку держави, його економічний потенціал і положення в світовій спільноті. Так, за деякими даними, об'єм витрат на розвиток інформаційної сфери в США сьогодні перевищує витрати на розвиток паливно-енергетичного комплексу цієї країни. [1]

В даний час відбувається стрімкий розвиток глобального процесу інформатизації суспільства. При цьому кардинальним чином змінюється все інформаційне середовище суспільства. Нові автоматизовані інформаційні технології проникають практично у всі сфери соціальної практики і стають невід'ємною частиною нової, інформаційної культури людства. [1]

Інформаційна технологія – це технологія обробки даних (інформаційного ресурсу), яка складається з сукупності

технологічних елементів: збирання, накопичення, пошуку, обробки, передачі даних користувачам на основі сучасних технічних засобів. [2]

Україна за рівнем розвитку інформаційних технологій у світі посідає 75 місце (дані 2011). Такі дані оприлюднила міжнародна громадська організація Всесвітній економічний форум у своїй шостій щорічній доповіді. У попередньому рейтингу Україна займала 76 позицію. Єдина конкурентна перевага, яку мас наша країна в цьому аспекті, це традиційно сильні ІТ-Кадри, тобто в Україні дуже високий рівень підготовки програмістів. Україна є одним зі світових центрів офшорного програмування. [3]

Застосування ІТ дозволило представити у формалізованому вигляді, придатному для практичного використання, концентрований вираз наукових знань і практичного досвіду для реалізації і організації соціальних процесів. При цьому відбувається економія витрат праці, часу, енергії, матеріальних ресурсів, необхідних для здійснення цих процесів. Тому ІТ грають важливу стратегічну роль, яка швидко зростає. Це пояснюється рядом їх властивостей:

- ІТ дозволяють активізувати і ефективно використовувати інформаційні ресурси суспільства, що економить інші види ресурсів – сировину, енергію, корисні копалини, матеріали, устаткування, людські ресурси, соціальний час.
- ІТ реалізують найбільш важливі, інтелектуальні функції соціальних процесів.
- ІТ дозволяють оптимізувати і у багатьох випадках автоматизувати інформаційні процеси в період становлення інформаційного суспільства.
- ІТ забезпечують інформаційну взаємодію людей, що сприяє розповсюдженню масової інформації. Вони швидко асимілюються культурою суспільства, знімають багато соціальних, побутових і виробничих проблем, розширюють внутрішні і міжнародні економічні і культурні зв'язки, впливають на міграцію населення по планеті.
- ІТ займають центральне місце в процесі інтелектуалізації суспільства, в розвитку системи освіти, культури, нових (екранних) форм мистецтва, в популяризації шедеврів світової культури, історії розвитку людства.
- ІТ грають ключову роль в процесах отримання, накопичення, розповсюдження нових знань. Перший напрям – інформаційне моделювання – дозволяє проводити «обчислювальний експеримент» навіть в тих умовах, які

неможливі в натуральному експерименті із-за небезпеки, складності, дорожнечі. Другий напрям, заснований на методах штучного інтелекту, дозволяє знаходити вирішення завдань, що погано формалізуються, завдань з неповною інформацією, з нечіткими початковими даними. Мова йде про створенні метапроцедур, які використовуються людським мозком. Третій напрям – засновано на методах когнітивної графіки – сукупності прийомів і методів образного представлення умов завдання, які дозволяють відразу побачити рішення або отримати підказку для його знаходження. Воно відкриває можливості пізнання людиною самого себе, принципів функціонування своєї свідомості. [1]

Література:

1. Сучасні інформаційні технології в науці та освіті – 2016. / Вінницький національний технічний університет – Вінниця 2016 1-14с.

[Електронний ресурс]. URL:

http://sukhorukov.vk.vntu.edu.ua/file/SITNO/0adb2500d2f4abff939d80a7f4f5c11b.pdf

2. Г.Г.Швачич, В.В.Толстой, Л.М.Петречук, Ю.С.Іващенко, О.А.Гуляєва, Соболенко О.В. Сучасні інформаційно-комунікаційні технології: Навчальний посібник. – Дніпро: НМетАУ, 2017. –7с.

3. Сучасні інформаційні технології і Україна. [Електронний ресурс]. URL: http://megalib.com.ua/content/2054_91_Sychasni_informaciini_tehnologii_i_Ykraina.html

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Захаренков Андрій Олексійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Телекомунікаційні та інформаційні системи включають дротові та бездротові локальні та глобальні мережі та апаратне та програмне забезпечення, що забезпечує можливості систем для взаємодії між собою або з користувачами.

Набір телекомунікаційних систем, що підтримують більшість федеральних державних установ, включає мережеву інфраструктуру та інші компоненти технічних рішень, що належать комерційним провайдерам телекомунікаційних послуг і управляються від імені уряду. Залежності від постачальників телекомунікаційних систем піднімають особливі проблеми планування на випадок непередбачених ситуацій для власників систем, на які слід звернути увагу ISCP, наприклад, чи буде той самий чи окремий постачальник відповідати за надання альтернативних телекомунікаційних послуг, якщо основна послуга стане недоступною. Стратегії планування на випадок

надзвичайних ситуацій для телекомунікаційних систем включають:

1. Використання результатів аналізу впливу на бізнес для визначення непередбачених вимог щодо обслуговування або відновлення телекомунікаційних послуг.

2. Документування телекомунікаційної інфраструктури та послуг за допомогою фізичної та логічної мережі або архітектурних діаграм.

3. Документування інформації про конфігурацію системи, імен та контактної інформації провайдерів телекомунікацій та домовленостей про рівень обслуговування операцій на випадок непередбачених ситуацій.

4. Узгодження рішень на випадок непередбачених ситуацій з політиками безпеки мережі та засобами контролю, щоб забезпечити адекватні запобіжні заходи проти відключень мережі та інших збоїв.

Планування дій на випадок непередбачених ситуацій для телекомунікаційних систем має прагнути уникнути окремих точок відмови шляхом впровадження надмірних ліній зв'язку, мережевих пристроїв і навіть постачальників послуг. На додаток до резервування мережі та постачальника, можливості, що надаються телекомунікаційними системами для нормальної роботи, можуть забезпечити рішення на випадок непередбачених ситуацій, коли сайти первинної обробки або допоміжні компоненти інфраструктури недоступні. Такі можливості включають послуги віддаленого доступу для системних адміністраторів та іншого уповноваженого персоналу та технологію бездротових мереж як альтернативний або резервний механізм зв'язку під час зриву, що зачіпає локальну мережу або інші дротові мережеві компоненти. Інформаційній технології мають наступні властивості:

1. Високий ступінь розчленованості процесу на стадії, що відкриває нові можливості для його раціоналізації і перекладу на виконання за допомогою машин. Це - найважливіша характеристика машинного технологічного процесу;

2. Системна повнота (цілісність) процесу, що повинний включати весь набір елементів, що забезпечують необхідну завершенность дій людини при досягненні поставленої мети;

3. Регулярність процесу й однозначність його фаз, що дозволяють застосовувати середні величини при їхній характеристиці, і, отже, що допускають їхню стандартизацію й уніфікацію. У результаті з'являється можливість обліку, планування, диспетчеризації інформаційних процесів.

Інформаційні технології визначають способи, методи та засоби збору, реєстрації, передачі, зберігання, обробки та видачі (розповсюдження або публікації) інформації в інформаційних системах. Інформаційні технології відповідають на питання “як” та “за допомогою чого”. Принципова відмінність інформаційних технологій від технології виробництва полягає в тому, що вони містять елементи творчого характеру, тобто людський фактор, і не підлягають регулюванню та формалізації. Вирішення економічних та управлінських проблем завжди пов’язане із здійсненням дій щодо збору необхідної інформації, обробки її за деякими алгоритмами та передачі у зручній формі особі, яка приймає рішення. Ця традиційна технологія вирішення економічних та управлінських проблем називається предметною технологією. Залежно від технологічних засобів вирішення різних проблем певної предметної області можна ввести поняття забезпечення інформаційних технологій, подальший розвиток яких веде до поняття функціональної технології.

Оскільки інформаційні технології - це комбінація процедур, що реалізують функції збору, накопичення, зберігання, обробки та передачі даних за допомогою технічних засобів, отже, інформаційні технології нерозривно пов’язані з технічним та програмним середовищем, в якому вони реалізовані. Інформаційні технології залежать від різних компонентів, зокрема:

1. Технічних засобів;
2. Персоналу, здатного використовувати їх;
3. Організації, яка об’єднує засоби і персонал в єдиному процесі;
4. Інформаційних засобів, що здійснюють формування й видачу інформації.

Основою технології обробки даних є процеси перетворення вхідної інформації у вихідну. Кожна інформаційна технологія закінчується створенням інформаційного продукту. Підходи до класифікації інформаційних технологій значною мірою залежать від можливостей програмного та апаратного забезпечення комп’ютерів та телекомунікацій, предметної області їх застосування, цілей користувачів та завдань, які вони вирішують.

Класифікація інформаційних технологій у галузі економіки, бізнесу та управління може базуватися на таких класифікаційних ознаках, які дозволяють вибирати з безлічі можливих окремих груп інформаційних технологій.

Відповідно до мети та характеру використання, завдяки тому, що інформаційні технології можуть суттєво відрізнятися в

різних предметних областях та комп'ютерних середовищах, можна виділити два основних класи інформаційних технологій: забезпечуючі та функціональні інформаційні технології.

Процес надання інформаційних технологій - це технологія обробки інформації, яка може бути використана як інструмент у різних предметних областях для вирішення широкого кола проблем роботи з різними видами інформації. Ці технології залежать від типу інформації, яка обробляється (буквено-цифрові, табличні, графічні, аудіо, відео, віртуальна реальність). Це включає технології обробки текстів, електронні таблиці, бази даних, мультимедійні продукти, розпізнавання символів, телекомунікації, захист інформації та захист інформації, розробку програмного забезпечення тощо. Постачання технологій може базуватися на абсолютно різних апаратних та програмних платформах. Тому при їх поєднанні на основі предметної технології виникає проблема системної інтеграції, яка полягає у необхідності побудови різних інформаційних технологій до єдиного стандартного інтерфейсу. Прикладом цього можуть бути, наприклад, офісні комплекти MS Office та Open Office, які, незважаючи на свої природні відмінності, в основному функціонально ідентичні.

Функціональні інформаційні технології - це технології, що реалізують стандартні інформаційні процеси для вирішення проблем у певній предметній області та засновані на відповідних інформаційних технологіях. Призначення функціональних інформаційних технологій полягає в автоматизації виробничої діяльності фахівців у відведеному районі. Іншими словами, така модифікація забезпечується інформаційними технологіями, в яких реалізована будь-яка із предметних технологій, і є функціональною інформаційною технологією.

Таким чином, сприяючі та функціональні технології взаємопов'язані, наприклад, забезпечують технології для створення текстових документів, аналізу даних у електронних таблицях тощо можуть служити основою для функціональних інформаційних технологій: фінансових, офісних, освітніх, промислових тощо.

Тип інтерфейсу користувача може бути використаний як ознака класифікації, що зумовлює можливість користувача отримувати доступ до інформації та обчислювальних ресурсів при реалізації інформаційних процесів під час вирішення проблем користувача. Інтерфейс користувача розуміється як набір інструкцій, правил та програмного та апаратного забезпечення, що забезпечують взаємодію користувача з обчислювальною системою. Тип інтерфейсу користувача

залежить від типу операційної системи (однопрограмна, багатопрограмна, багатокористувацька мережа) та від технології обробки комп'ютерної системи. Використання цієї класифікаційної ознаки дає можливість виділити наступні типи інформаційних технологій.

Упаковані інформаційні технології характеризуються тим, що інформаційні процеси здійснюються у визначеній послідовності і не вимагають втручання користувача. У цьому випадку завдання або раніше накопичені дані за певними критеріями об'єднуються в пакет для подальшої автоматичної обробки відповідно до зазначених пріоритетів. Користувач не може впливати на хід виконання завдань під час обробки пакету, його функції обмежуються підготовкою вихідних даних про комплекс завдань та передачею їх до обробного центру. В даний час пакетний режим реалізований щодо електронної пошти та звітності в суворо формалізованій формі.

Інформаційні технології діалогу надають користувачам необмежену можливість інтерактивної взаємодії з інформаційними ресурсами в режимі реального часу, отримуючи при цьому всю необхідну інформацію для вирішення функціональних проблем та прийняття рішень. Ці технології передбачають відсутність жорстко фіксованої послідовності операцій перетворення даних та активну участь користувача, аналіз проміжних результатів та генерування команд управління в процесі обробки інформації.

Якщо однопрограмні операційні системи (наприклад, MS DOS) дозволяють організувати пакетну або інтерактивну інформаційну технологію, то багатопрограмні операційні системи (наприклад, сімейство Windows) можуть поєднувати свої програми.

Мережеві інформаційні технології забезпечують користувачеві доступ до географічно розподіленої інформації та обчислювальних ресурсів за допомогою спеціальних засобів зв'язку. Вони реалізовані мережевими (багатокористувацькими) операційними системами (наприклад, Windows NT / 2000/2003, Linux), забезпечуючи як мережеві, так і пакетні та розмовні інформаційні технології. У цьому випадку користувачі мають можливість використовувати дані, накопичені на інших робочих місцях, перерозподілити обчислювальну потужність між процесами вирішення різних функціональних завдань, а також можливість спільного вирішення однієї проблеми кількома користувачами.

Використання сучасних комп'ютерних технологій в Україні поступово перетворюється на потужний ЗМІ, здатний

дуже ефективно впливати на формування громадської думки, миттєво поширюючи інформацію, дані та навіть визначати поведінку людей. Тому доцільно, щоб контроль над ним проводився на постійній основі.

Література
1. *R. Biadacz. The Use of Modern Information Technology 2015.*
2. *Carne, E. Bryan Modern Telecommunication 2019.*
3. *D. Power, R. Hadidi. Modern Information Systems: Expanding the Boundaries 2018.*

ПОКРАЩЕНЕ РОЗПІЗНАВАННЯ КОНТЕКСТНОЇ ІНФОРМАЦІЇ ДЛЯ СТВОРЕННЯ ІНДИВІДУАЛЬНОГО ЕЛЕКТРОННОГО ОБРАЗУ КОРИСТУВАЧА НА ПРИКЛАДІ МУЗИЧНИХ ВПОДОБАНЬ

Ігнатова Марія Володимирівна, Леньо Володимир Ярославович
Державний університет телекомуннікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Прогрес склався так, що за останню декаду технології збору інформації сягнули небувалого раніше прогресу у визначенні індивідуальних уподобань кожного окремо взятого користувача сервісу. До сих пір розвиток йшов у сторону розпізнавання голосу людини, але недавній патент включає обробку також таких контекстних даних голосового запиту, як: настрій особи, вік, стать, акцент, фізичне середовище (автобус, метро, поїзд, вулиця, школа, парк і так далі), соціальне середовище (чи людина одна, чи знаходиться в невеличкій групі, на вечірці, тощо) – а також опирається на історію прослуховувань та на музичний смак друзів. Це стає одним з декількох факторів, що впливають на електронний образ користувача, а таким чином і на рекомендації, а також, що найголовніше для бізнесу, на зацікавленість споживача у продукції та послугах [1].

Як ми знаємо, кожен має особисті музичні уподобання, які, як показують дослідження, залежать від характеру людини [2]. Наприклад, статистика показує, що ті, хто слухають метал та рок, схильні бути більш інтровертивними, а фанати поп музики та репу, навпаки, більш відкриті та комунікабельні. Дослідницька група Spotify дійшла до висновку, що більш прискіпливі та роботящі люди концентруют прослуховування музики у вузьких проміжках часу [2].

Ця технологія реалізується так: система отримує звукові дані, фільтрує та форматує їх, розпізнає мову – а потім алгоритм визначає метадані: емоційний стан людини, стать, вік, акцент, середовище. Після цього метадані нормалізуються, тобто з розпізнаної мови видаляються дублікати слів, вставні слова та слова паразити, та дані накінець оброблюються пошуковою системою.

Більш широко, ці дані також включаються у глобальніший алгоритм, що звертає увагу також на історію прослуховувань та пошуку користувача, на музику, яка раніше сподобалася користувачу, на попередні метадані з голосового введення, а також чому віддають перевагу користувачі зі списку друзів.

Якщо же таких метаданих немає, тобто користувач у системі недавно та ще не встиг залишити ніякого сліду, то система буде рекомендувати на основі популярних пісень глобально або ж орієнтуючись на системну мову користувача та, якщо можливо, на його місцезнаходження.

Література:

1. Офіційний сайт компанії BBC [Електронний ресурс] - https://research.atspotify.com/just-the-way-you-are-music-listening-and-personality/

2. Офіційний блог R&D підрозділу компанії Spotify [Електронний ресурс] - https://research.atspotify.com/just-the-way-you-are-music-listening-and-personality/

БЕЗПІЛОТНІ КУР'ЄРИ. ДОСТАВКА МАЙБУТНЬОГО?

Ігнатова Марія Володимирівна

Леньо Володимир Ярославович

Державний університет телекомуннікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Останній рік видався досить важким для всього світу. І в умовах пандемії багато галузей інформаційних технологій знайшли свій варіант розвитку саме в первинних потребах людства. Протягом 2020 року активно стали розвиватися і отримувати нові можливості в експлантації роботи-безпілотники.

Робот-кур'єр - це безпілотний механізм (рідше керований дистанційно), який доставляє товари, замінюючи людину-кур'єра. Найчастіше це невеликі вантажі.

Ідея розвитку безпілотного кур'єра далеко не нова і ще з часів, коли смартфон здавався задумкою фантаста, думки про подібного роду технології були. Але, все ж таки, до активної розробки безпілотних кур'єрів світ прийшов не так вже й давно, а всього кілька років тому.

У 2018 році екс-інженери компанії Google відкривають свій стартап - безпілотний автомобіль Nuro[1].

Автономна модель тоді отримала назву Nuro R1.Це невеликий автоконтейнер на колесах.

За «зір» смарт-мобіля відповідає лазерна система Lidar, датчики, радари і відеокамери, які встановлені на даху машини. У моделі повністю відсутні місця для водія і пасажирів, тому він оснащений тільки відсіками для товарів. При доставці товару клієнти отримують через мобільний додаток спеціальний код,

який і дозволяє відкрити автомобіль і отримати придбані покупки. Подібна технологія подалі буде використана іншими компаніями в роботі доставщиків.

Уже в 2019 році з'являлося все більше компаній зі своїми роботами-кур’єрами: Refraction AI [2], Agility Robotics [3], starship [4] та інші.

З початком 2020 року подібні сервіси стали необхідні ще більше і їх розвиток тільки посилився. Якщо раніше безпілотні кур'єри здебільшого розглядалися в США і Британії, то з початком пандемії така технологія знайшла своє місце й в інших країнах : Китаї (neolix [4]), Франції (twinswheel), Росії (Яндекс Доставці), Південній Кореї та інш.

Експерти стверджують, що є дві основні проблеми, які необхідно вирішити, перш ніж робо-кур’єри стануть звичайним явищем на вулицях світу.

Перша - це безпека. Хоч пристрої і оснащені достатньою кількістю технологій, які допомагають їм орієнтуватися в просторі. Більшість країн все ще вважають цю технологію не безпечною.

Друга - ціна. На такого робота і його обслуговування вона все ще залишається досить високою. І питання що ж вигідніше робот або людина є відкритим.

Але, навіть при наявності таких нюансів, в 2021 році ми цілком можемо очікувати активне зростання застосування подібних робо-кур’єрів по всьому світу, особливо в країнах, де нові технології впроваджуються швидше за все, наприклад як США, Японія, Китай і Західна Європа.

Що стосується України. В нашій країні поки немає основної фірми, що займається цим питанням і впроваджує безпілотну доставку, але судячи з розвитку цих технологій в світі, можна судити, що скоріш за все ми почуємо про успіхи впровадження подібного роду доставки в найближчому майбутньому.

Література:

1. Офіційний блог компанії Nuro [Електронний ресурс] -https://medium.com/nuro

2. Офіційний сайт компанії Refraction.Ai [Електронний ресурс]- https://refraction.ai/

3. Офіційний сайт компанії Starship[Електронний ресурс]- https://www.starship.xyz/

4. Офіційний сайт компанії Neolix[Електронний ресурс]- https://www.neolix.cn/productCenter.html

ОСНОВНІ ПРОГРАМИ ДЛЯ ВІДЕОМОНТАЖУ

Кас'яненко Ігор Олександрович

Державний університет телекомунікацій
Навчально-науковий інститут Телекомунікацій
м. Київ

В сучасному світі люди все більше приділяють час перегляду відеороликів різного формату, що веде до все більшого використання нових можливостей обробки відео різними програмами. На даний момент існують деякі програми, які можуть забезпечити не просто редагування відео, а й зробити навіть міні-фільм в домашніх умовах. Тут будуть розглянуті лише найбільш популярні програми.

Movavi Video Suite

Вона не має великої популярності серед користувачів, в порівнянні з більш дорогими аналогічними сервісами, але це не робить її менш якісною. Основним плю-сом Movavi Video Suite є велика кількість різноманітних функцій.

Основні функціональні можливості програми Movavi Video Suite:

- простий і зрозумілий російськомовний інтерфейс;
- різноманіття візуальних ефектів для обробки відеоряду;
- можливість точного налаштування візуальній складовій;
- можна монтувати об'єкти в різних форматах;
- наявність конвертера для відео, звукозапису, картинок;
- різні функції для звукозапису; підтримує технологію NVIDIA CUDA;
- оптимізація під екрани смартфонів;
- експорт в Youtube, ВКонтакте тощо з самої програми для відеомонтажу;
- висока швидкість роботи;
- софт постійно оновлюється, з'являються нові опції;
- безкоштовна робота в тестовому періоді.

Adobe Premiere Pro

Вона є однією з найпопулярніших професійних програм для відеомонтажу серед подібних платформ. Її часто застосовують для роботи голлівудські фахівці. У неї входять численні різноманітні опції і спецефекти.

Основні якості і функції програми Adobe Premiere Pro:

- можна працювати в режимі реального часу;
- є версія російською мовою, оновлення та підтримка від компанії Adobe;
- точна настройка колірної гами, контрасту і т.д;
- висока якість монтажу відеоряду та звукового запису;
- наявність функції нелінійного монтування;
- різноманіття всіляких фільтрів і ефектів;
- наявність мультитрековий режиму;

- підтримка численних форматів;
- можливість здійснювати захоплення відео з різних джерел;
- опція триммінгу, яка допомагає більш точно підганяти кадри при монтажі;
- можна застосовувати одночасно відеоряд різної якості;
- наявність кодувальника Adobe Media Encoder;
- пробна безкоштовна версія на 30 днів.

Sony Vegas Pro

За допомогою неї часто монтують свої відеороботи творці телесеріалів, коротких фільмів, веб-розробники та інші професіонали. Також існує простіша версія для новачків в цій сфері - VEGAS Movie Studio.

Можливості та функції Sony Vegas Pro:

- різноманіття ефектів, аудіо налаштувань, шаблонів, фільтрів і т.д;
- обробка відеоряду з дозволом до 4096x4096;
- багатодоріжковий монтаж в високій якості;
- опція абсолютної відсутності сторонніх звуків; робота в різних форматах;
- можливість відкриття гігапіксельних картинок;
- налаштування колірної гами;
- високу професійну якість устаткування, що монтується відео і звукоряду;
- наявність опції картинка в картинці;
- обробка в режимі реального часу;
- можливість здійснювати захоплення відео з різних джерел:
- файли, диски, камери, екрану і т.д.

Pinnacle Studio

Вона буде зручна в тому числі для домашніх умільців. Її функціонал не гірше, ніж у продукту від Adobe, але стиль роботи, меню і візуалізація дещо відрізняються.

Основні функціональні можливості програми Pinnacle Studio:

- інтуїтивне управління;
- пакети на вибір (pinnacle studio базова, розширена plus і максимальна ultimate);
- більше 2000 ефектів і переходів для відео, аудіо;
- функція keying;
- можливість оцінити використаний ефект у вікні попереднього перегляду;
- вбудована програма редагування відео титрів;

- широкі можливості запису відео в кінці роботи (веб, hd, avi і т.д.);
- запис результуючого звуку у форматі dolby digital 5.1.

Висновки:

Я використовував програму Sony Vegas Pro, але перейшов на Adobe Premiere Pro (спочатку на версію 2017-го року, на даний момент користуюсь версією 2020-го). Дана програма має все, що потрібно для роботи з моїми проектами та завданнями, проте слід зазначити, що вона дуже тяжка для системи та потребує багато ресурсів.

Із явних недоліків, які я помітив у це Adobe Premiere Pro:

- ціна ліцензії доволі велика(є багато піратських взломаних версій);
- різні помилки програми(російська версія та назви на ній вхідних файлів).

Література:

1. *http://www.smilefilm.lviv.ua/smilefilm/top-5-program-dlya-videomontazy/*
2. *https://seo-akademiya.com/baza-znanij/kontent/programmyi-dlya-montazha-i-obrabotki-video/*

ПРОГНОЗ ЗРОСТАННЯ ІНТЕРНЕТ-ТРАФІКУ

Клименко Ніката Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Більшість тенденцій телекомунікаційної галузі говорять про її розвиток, масштабування і глобальному проникненні інтернет технологій в усі галузі життя. Незалежні аналітики пророкують стрімке зростання трафіку в найближчі роки. Пояснюють це розвитком технологій і збільшенням числа інтернет-користувачів, як наслідок, збільшення навантаження на мережі операторів, масове впровадження об'єктів Інтернету речей, примноження кількості підключених до мережі гаджетів, користувачів, використання різного роду додатків, «розгін» швидкості передачі даних і т.д.

За даними Cisco за останні два десятиліття обсяг інтернет-трафіку істотно зріс. З 1992 по 2017 роки денний обсяг зріс з 100 ГБ до 45 000+ ГБ. А до 2022 року світ чекає триразове збільшення інтернет трафіку.

Щорічні прогнози Cisco засновані на думках аналітиків-експертів, власних оцінках і прямому зборі даних.

За колишніми прогнозами в період 2013-2018 рр. кількість мобільних користувачів мала збільшитися до 4,9 млрд чоловік. За даними Hootsuite на 2019 рік їх число відповідає 5,1 млрд.

Мобільному відео передбачали захоплення 69% світового інтернет трафіку. У 2019 другим за відвідуваністю ресурсом визнаний YouTube. Щомісячне число відео-глядачів - 92% користувачів, або 4 млрд осіб.

У 2022 році на одну людину доведеться 3,6 онлайн-пристроїв (в цілому 28,5 млрд). Розподіл трафіку за типами пристроїв виглядає так:

- 71% - бездротові і мобільні, з них 44% на смартфони;
- 29% - дротяні, з них 19% на ПК.

Аналіз прогнозу світових лідерів надання телекомунікаційних послуг показав, що 82% від світового трафіку займе відео і 17% припаде на лайф-відео. Інтернет-відео на ТБ зросте втричі, до 27% від фіксованого відео-трафіку. Удвічі додасться споживчий трафік відео за запитом, що відповідає 10 млрд DVD-дисків на місяць.

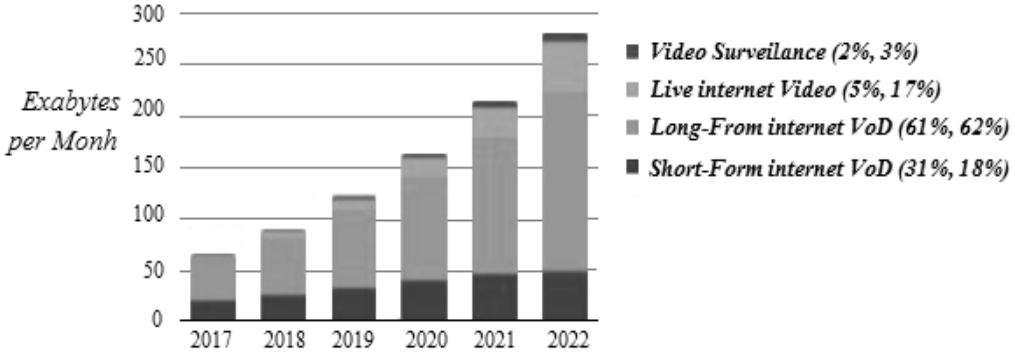


Рис. 1 - Глобальне інтернет-відео по підсегментам

Трафік інтернет-ігор виросте на 55%, а трафік віртуальної і доповненої реальності - на 65%.

Серед основних тенденцій:

1) Поєднання різноформатних пристроїв і різнотипних з'єднань. До 2022 року 81% IP-трафіку і інтернет-трафіку доведеться на пристрої, що не відносяться до ПК.

2) Перехід від середовища IPv4 до середовища IPv6. Завдяки цьому стає можливим підключення до Інтернету речей (IoT). До 2022 року 64% усіх стаціонарних і мобільних мережевих пристроїв перейдуть на IPv6, в порівнянні з 32% в 2017 році.

3) Посилення зростання IoT за рахунок додатків M2M. Інтернет речей поступово об'єднує людей, предмети, процеси і дані. До 2022 року на кожну людину буде підключено 1,8 M2M з'єднання.

До головних трендів відносяться:

1. Зростання трафіку додатків. До 2022 року загальна частка всіх форм IP-відео, що передаються відеофайлів, відео-потокових ігр та відеоконференцій становитиме 80-90% від загального IP-трафіку.

2. Пріоритет інтернет-відео над традиційним ТВ. Обсяг трафіку по інтернет-ТБ зросте на 72%.

3. Посилення уваги до онлайн-безпеки. При цьому до 2022 року загальна кількість DDoS-атак збільшиться вдвічі і досягне 14,5 млн.

4. Збільшення швидкості інтернет-доступу. Середньостатистична швидкість на 2022 рік складе 75,4 Мбіт / с проти 39,0 Мбіт / с в 2017 році.

5. Поширення Wi-Fi технологій. У 4 рази зросте кількість громадських точок доступу Wi-Fi, до 549 млн до 2022 року.

В цілому очікуваний обсяг глобального інтернет-трафіку складе 4,8 ZB в рік (1,9+ трлн ГБ). Щомісячний IP-трафік на душу населення зросте з 16 ГБ до 50 ГБ, що призводить до необхідності виконувати класифікацію інтернет трафіку для управління такими технологіями, як мережева безпека, диференціація сервісів, управління параметрами трафіку і ін.

Література:

1. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper.

2. Степутин А.Н., Николаев А.Д. Мобильная связь на пути к 6G. Том 2./ А.Н. Степутин, А.Д. Николаев. –Волог:Инфра-Инженерия, 2017.-416с.

ШТУЧНИЙ ІНТЕЛЕКТ

Клінков Олександр Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Коли люди у фільмах бачать роботів, вони думають, що це штучний інтелект. Насправді штучний інтелект – це набір математичних моделей, які натреновані для аналізу і класифікації даних.

Якщо більш детально розглянути ці моделі, то крім статистики і теорії ймовірності в ШІ застосовується математична логіка, матричне числення, методи оптимізації, різні математичні перетворення. Для того, щоб реалізувати ці моделі потрібен комп'ютер. Це може бути персональний комп'ютер, мікропроцесори в роботах і мобільних гаджетах, сервери комп'ютерних мереж. Це означає, що для фахового впроваджування застосунків ШІ випускнику крім математики потрібно мати знання в галузі комп'ютерних наук: знати архітектуру комп'ютера і комп'ютерних мереж, формати даних і методи обробки даних в інформаційних технологіях, вміти програмувати.

Сучасні великі компанії, наприклад, Google за рахунок надвеликих технічних можливостей комп'ютерів по об'єму

пам’яті і швидкодії, перевели ШІ на новий рівень, коли системи ШІ навчаються на мільйонах прикладів, самі системи складаються з сотень блоків і технічно це реалізується на суперкомп’ютерах серверних і хмарних технологіях.

Успіх практичного застосування методів ШІ залежить не тільки від володіння теоретичними знаннями, але у великій мірі від вміння правильно застосовувати методи моделювання і підготувати початкові дані, як кажуть, щоб дані були репрезентативними.

Банки застосовують системи штучного інтелекту в страховій діяльності при грі на біржі і управлінні власністю. У серпні 2001 року роботи виграли в людей в імпровізованому змаганні з трейдингу. Методи розпізнавання образів, (включаючи, як складніші й спеціалізованіші, так і нейронні сітки) широко використовують при оптичному і акустичному розпізнаванні (в тому числі тексту і голосу), медичній діагностиці, спам-фільтрах, в системах ППО, а також для забезпечення ряду інших задач національної безпеки.

Застосування ШІ є важливим трендом у створенні перспективних систем управління поля бою та озброєнням.

За допомогою ШІ можливо забезпечити оптимальний та адаптивний до загроз вибір комбінації сенсорів і засобів ураження, скоординувати їх сумісне функціонування, виявляти та ідентифікувати загрози; оцінювати наміри противника. Суттєву роль ШІ відіграє у реалізації тактичних систем доповненої реальності. Наприклад, ШІ дозволяє забезпечити класифікацію та семантичну сегментацію зображень, локалізацію і ідентифікацію мобільних об'єктів з метою схематичного відтворення контурів об'єктів в якості символів доповненої реальності для ефективного цілевказування.

В книзі «AI. Наддержави штучного інтелекту» відомий фахівець з розпізнавання мови Кай-Фу Лі прогнозує: «Першим світ підкорить штучний інтелект інтернету, потім штучний інтелект для бізнесу, потім настане черга для штучного інтелекту сприйняття і автономного штучного інтелекту. На кожному з цих етапів штучний інтелект буде захоплювати нові сфери повсякденного життя людей». Таким чином, розуміння суті ШІ, вміння ним користуватись є дуже важливим для фахівця з інформаційних технологій.

Література:

1. https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82

РОЗШИРЕНА РЕАЛЬНІСТЬ

Клінков Олександр Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Розширена реальність – це технологія, яка розширює наш фізичний світ, додаючи до нього шари цифрової інформації. На відміну від віртуальної реальності (VR), AR не створює цілих штучних середовищ, щоб замінити реальну віртуальну. AR з'являється під прямим переглядом існуючого середовища та додає до нього звуки, відео, графіку.

Погляд на фізичне реальне середовище із накладеними комп'ютерними зображеннями, що цим самим змінює сприйняття реальності, і є AR.

Сам термін був введений ще в 1990 році, і одними з перших комерційних застосувань були телебачення та військові потреби. З розвитком Інтернету та смартфонів AR розгорнула свою другу хвилю популярності і в наш час пов'язана з інтерактивною концепцією. 3D-моделі прямо проектуються на фізичні речі або з'єднуються разом у режимі реального часу. Різні додатки для доповненої реальності впливають на наші звички, соціальне життя та індустрію розваг.

Програми AR зазвичай накладають цифрову анімацію до спеціального "маркера" або за допомогою GPS у телефонах, що визначають місцеположення. Доповнення відбувається в режимі реального часу та в контексті навколишнього середовища. Наприклад, накладання результатів на спортивні змагання в прямому ефірі.

Сьогодні існує 4 типи доповненої реальності:

- безмаркерова AR;
- маркерна AR;
- проекційна AR;
- AR на основі нашарування;

Для AR може використовуватися певний діапазон даних (зображення, анімація, відео, 3D-моделі), і люди будуть бачити результат як в природному, так і в синтетичному світлі. Крім того, користувачі знають, що вони знаходяться в реальному світі, який просто доповнений комп'ютером, на відміну від віртуальної реальності (VR).

AR може відображатися на різних пристроях: екранах, окулярах, кишенькових пристроях, мобільних телефонах, наголовна дисплеях. Вона включає в себе такі технології, як S.L.A.M. (Одночасна локалізація і відображення), відстеження глибини (дані датчика, що обчислюють відстань до об'єктів), а також такі компоненти:

1) **Камери і датчики.** Збір даних про взаємодію користувачів і відправка їх для обробки. Камери на пристроях сканують оточення, і за допомогою цієї інформації пристрій знаходить фізичні об'єкти і генерує 3D-моделі. Це можуть бути камери спеціального призначення, як, наприклад, в Microsoft Hololens, або звичайні камери смартфонів для фото і відео.

2) **Обробка.** В кінцевому підсумку пристрої AR повинні діяти як маленькі комп'ютери, як це вже роблять сучасні смартфони. Точно так же вони вимагають процесора, графічного процесора, флеш-пам'яті, ОЗУ, Bluetooth / WiFi, GPS і т.д., щоб мати можливість вимірювати швидкість, кут, напрям, орієнтацію в просторі.

3) **Проекція.** Це відбувається за допомогою мініатюрного проектора на гарнітурах AR, який приймає дані від датчиків, обробляє їх і виводить на поверхню для перегляду. Фактично, використання проекцій в AR ще не повністю розроблено так, щоб його можна було використовувати в комерційному середовищі: товарах або послугах.

4) **Відображення.** У деяких пристроїв AR є дзеркала, які допомагають людському оку переглядати віртуальні зображення. У деяких є масив маленьких вигнутих дзеркал, а у деяких – двостороннє дзеркало, що відбиває світло від камери і очей користувача. Метою таких траєкторій відображення є правильне вирівнювання зображення.

Доповнена реальність може доповнювати нашу повсякденну діяльність різними способами. Одними з найпопулярніших використанням додатків AR є ігри. Нові AR ігри покращують призначені для користувача можливості для гравців, деякі з них навіть сприяють більш активному способу життя (Pockemon Go, Ingress). Ігрові майданчики переміщаються з віртуальних сфер в реальне життя, і гравці фактично виконують певні дії в фізичному світі. AR в роздрібній торгівлі може вплинути на залучення і утримання клієнтів, а також впізнаваність бренду і збільшення продажів. Деякі функції також можуть допомогти замовникам зробити свої покупки, засновані на надання даних про продукти з 3D-моделями будь-якого розміру або кольору. Ринок нерухомості також може скористатися перевагами доповненої реальності за допомогою тривимірних екскурсій по квартирах і будинках.

Література:

1. *http://teach-hub.com/scho-take-dopovnena-realnist/*
2. *https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BF%D0%BE%D0%B2%D0%BD%D0%B5%D0%BD%D0%B0_%D1%80%D0%B5%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C*

ЗРУЧНІСТЬ СПІЛКУВАННЯ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ПРОДУКТУ

Ковбаса Віталій Вікторович
Інститут Інформаційних технологій
Державний Університет Телекомунікацій
м. Київ

Розробка програмного забезпечення, для спілкування людей по інтересам та обміну інформацією між ними, що розроблена за допомогою ReactNative. React Native - це фреймворк мобільних додатків з відкритим кодом, створений Facebook. Він використовується для розробки програм для Android, iOs, macOS,Web та Windows [2].

Є програми, які розраховані на застосування всередині локальної мережі компанії. Такі допомагають співробітникам спілкуватися між собою, спільно працювати над проектами і завданнями. Мессенджер - програма, яка дозволяє миттєво обмінюватися повідомленнями, з'єднуватися з іншими користувачами телефонними дзвінками та використовувати відео-зв'язок.

Найбільшу популярність і застосування отримали сервіси, доступні широкому колу користувачів. Залежно від країни, перелік улюблених месенджерів буде різним.

Мій проект - це всі популярні мессенджери в одному додатку. Це зручніше, ніж постійно переключатися з одного додатку на інший, особливо коли користувачу надсилають багато повідомлень. Також, це економія часу людини, а це дуже важливо.

Тайм-менеджмент- це ефективний інструмент, який може допомогти кожній працюючій людині зробити час її роботи максимально ефективним, залишивши сили і вільні години на відпочинок [3].

Отже, в даній роботі продемонстровано сучасний підхід до розробки програмних додатків ReactNative. Розроблений додаток- це зручність та допомога студентам, працівникам, користувачам економити свій час.

Література:
1. *IBMacadmy.pdf Marketingbuild-2018 Url: https://uploads/2018/imbacademy.pdf*
2. *Learning React Native: Building Native Mobile Apps with JavaScript*
Url: https://pepa.holla.cz/wpcontent/uploads/2016/12/Learning-React-Native.pdf
3. *Semantica. ContentMarketing-2019. URL: https://semantica.in/*

РОЛЬ ARDUINO В ДОДАТКАХ РЕАЛЬНОГО СВІТУ

Козлов Ілля Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У цій роботі досліджується принцип роботи і застосування плати Arduino nano. Тут також розглядається, як її можна використовувати в якості інструменту для досліджень і проектних робіт. Плата Arduino може надати швидкий інструмент в розробці випробувального стенду VLSI, особливо датчиків. Основні переваги - швидка обробка і зручний інтерфейс.

Сьогодні, коли число людей, які щодня використовують програмне забезпечення та обладнання з відкритим вихідним кодом, зростає, технології формують новий вимір, роблячи складні речі простіше і цікавіше. Ці відкриті джерела надають безкоштовні або практично недорогі, високонадійні і доступні технології.

Массімо Банзая, співзасновник Arduino, згадує кілька дуже важливих причин, чому потрібно використовувати саме Arduino?

1) Активне співтовариство користувачів: група людей, що використовують аналогічний продукт, може проводити бесіди у вигляді опублікованих повідомлень і ділитися своїм досвідом або вирішувати проблеми інших користувачів в спільнотах на власному досвіді [1]. «Якщо почати заряджати все, все дуже швидко вмирає» - каже Банзая, співзасновник Arduino.

2) Розвиток Arduino: Arduino був розроблений з метою надати любителям, студентам і професіоналам економічний і безпроблемний спосіб створення пристроїв, які взаємодіють з їх ситуацією за допомогою датчиків і виконавчих механізмів. Це робить його ідеальним для новачків, щоб швидко почати роботу [1].

3) Недороге обладнання: оскільки Arduino є платформою з відкритим вихідним кодом, програмне забезпечення не купується, і оплачуються тільки витрати на покупку плати або її частин, що робить її дуже дешевою. Проекти обладнання також доступні безкоштовно в Інтернеті на офіційному сайті [1].

4) Плата Arduino, як програміст: щоб спростити роботу плати Arduino, а також зробити її доступною всюди, ці плати поставляються з кабелем USB для забезпечення вимог до живлення, а також для роботи в якості програматора [1].

5) Мультиплатформенне середовище: Arduino IDE може працювати на декількох платформах, включаючи Microsoft, Linux і Mac OS X, що робить співтовариство користувачів ще більше [1].

Arduino, представлена в 2005 році, являє собою плату мікроконтролера з відкритим вихідним кодом. Це платформа,

яка дозволяє зацікавленим людям легко і дешево створювати електронні пристрої, які можна запрограмувати для взаємодії із зовнішнім середовищем за допомогою датчиків і виконавчих механізмів. Вона має безліч можливостей, таких як введення, висновок, обробка, отримання та відправка інформації через Інтернет. Розробники пишуть мови програмування C або C ++ в інтегрованому середовищі розробки Arduino (IDE) для програмування плати розробки Arduino. З плином часу було розроблено кілька версій обладнання Arduino, починаючи з базової Arduino-Uno, потім Mega, Mini, Nano, LilyPad та інших. Найменшим з них є Nano, як видно з його назви. Вона має характеристики, аналогічні платі Uno. Нові плати Nano маленькі, дешеві і підходять для невеликих проектів [3].

Тепер характеристики крихітних плат Nano краще за нижчою ціною. Arduino Nano Every і Nano 33 IoT, який додає безпроводовий зв'язок, доступні без заголовків за нижчою ціною. Вони можуть бути підключені до ланцюгів для взаємодії із зовнішнім середовищем, тобто датчикам, освітленням, двигунам, мікрофонам і т. ін. Нові чотири плати:

a) Arduino Nano Every для наших «повсякденних» проектів.

б) Arduino Nano 33 IoT (Інтернет речей) для проектів Інтернету речей.

c) Arduino Nano 33 BLE (Bluetooth з низьким енергоспоживанням) для підключення Bluetooth.

d) Arduino Nano BLE Sense, який включає безліч вбудованих датчиків [2].

Нові плати повинні мати модульну структуру. Ці плати призначені не тільки для великих виробників, але і для невеликих, які хочуть робити пристрої відповідно до своїх прототипів, заснованими на класичних платах або платах MKR. Ми можемо зробити висновок, що у споживачів буде більше можливості для розробки програмної частини, включивши ці плати в свої додатки або проекти в IoT, WSN, інтелектуальні пристрої.

Література:

1. ARDUINO.CC, “Arduino – Introduction”, 2015 [Online] Available: http://arduino.cc/en/Guide/Introduction. [Accessed: 25- Feb - 2015].

2. https://www.tomshardware.com/news/arduino-nano-boards-specs-every-iot-ble-sense,39371.html, [Accessed: 04- August- 2020].

3. https://fossbytes.com/arduino-nano-board-family-every-33-iot-ble/, [Accessed: 04- August- 2020].

СЕНСОРНА ГІПЕРПАНЕЛЬ ДЛЯ АВТОМОБІЛЯ MBUX

HYPERSCREEN

Коліда Володимир Петрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Представлений минулої осені новий Mercedes-Benz S-класу став першою моделлю з медіасистемою MBUX другого покоління, яка має великий сенсорний «планшет» для управління більшістю другорядних функцій машини. Але для флагманського електромобіля Mercedes-Benz EQS, який побачить світ в першій половині цього року, розробники підготували ще одну ітерацію цієї системи. Вона називається MBUX Hyperscreen і вже представлена окремо від автомобіля-носія на виставці CES-2021.

Hyperscreen - це одна велика скляна поверхня на всю ширину передньої панелі (141 см), яка об'єднує три дисплея і дефлектори вентиляції, але при цьому не має фізичних кнопок і перемикачів. Також в цей «гіперекран» вбудовані елементи контурної підсвічування салону. Поверхня площею 2432 см^2 має вигини, форма яких задається в процесі виготовлення при температурі 650 градусів, щоб уникнути спотворень. В систему інтегровано штучний інтелект для управління інформаційно-розважальними і транспортними функціями.

Гіперекран - ключовий елемент інформаційно-розважальної системи MBUX (Mercedes-Benz User Experience), в якій немає жодної фізичної кнопки. І він повинен вивести споживання контенту на абсолютно новий рівень.

Судячи з фото, в MBUX Hyperscreen відразу три дисплея на органічних світлодіодах (OLED), які вбудовані один великий, що охоплює всю панель, шматок вигнутого скла. За автоматичну оптимізацію яскравості у відповіді датчик освітленості і

спеціальна камера. Подивитися, як це все виглядає, можна в відео.

В основі системи тактильного зворотного зв'язку - дванадцять силових приводів. Підтримує роботу потужний комп'ютер з восьмиядерна процесором і 24 ГБ оперативної пам'яті, що відповідає за високу пропускну здатність.

В інтерфейсі медіасистеми передбачений так званий нульовий шар: в одній частині екрану завжди зібрані всі основні розділи меню, щоб забезпечити швидкий доступ. А ще розробники обіцяють «штучний інтелект», тобто програму самонавчання: мультімедійка зможе пропонувати ті чи інші функції, до яких водій або пасажир періодично звертаються.

В кінці 2021 року розпочнеться серійне виробництво Hyperscreen. Нагадаємо, що раніше компанія Mercedes-Benz розповіла про просунутої системі фільтрації для EQS, що робить повітря в салоні чистим як в операційному блоці. Автовиробник очікує, що його MBUX Hyperscreen «сформує абсолютно новий досвід взаємодії водія і переднього пасажира з авто».

Література:

1. https://mind.ua/ru/publications/20220850-ces-2021-10-vau-novinok-glavnoj-vystavki-elektroniki

2. https://autoreview.ru/news/elektromobil-mercedes-eqs-budet-imet-hyperscreen

3. https://blog.comfy.ua/v-mercedes-benz-predstavili-56-dyujjmovyjj-giperehkran-dlya-flagmanskogo-ehlektrokara-eqs/

СМАРТФОН З РОЗСУВНИМ ЕКРАНОМ LG ROLLABLE

Коліда Володимир Петрович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

У вересні 2020 року корейська корпорація LG анонсувала роботу над новим проектом. Менше, ніж за півроку, компанія продемонструвала унікальний смартфон з гнучким OLED-дисплеєм, здатним натисканням кнопки «розтягуватися» і перетворювати телефон в невеликий планшет.

Компанія не стала вдаватися в подробиці про перспективний смартфон, але представники підтвердили журналістам видання Engadget, що, коли він буде запущений, то буде називатися LG Rollable. Назва досить банальна, але вона відразу дає зрозуміти, про що йде мова: в складеному стані частина дисплея зможе скручуватися всередину корпусу.

LG Rollable виглядає привабливою відповіддю на безліч складних телефонів Samsung, але поки деталей мало. На відміну від Galaxy Z Fold 2, в якому високий і вузький зовнішній дисплей поєднується з широким внутрішнім дисплеєм, єдиний екран

Rollable має такий самий розмір, як традиційний дисплей смартфона, поки він не буде механічно розсунутий до розмірів невеликого планшета. Такий дизайн дозволить уникнути характерної складки, присутньої у багатьох існуючих складних рішень.

Пристрій буде використовувати гнучкий OLED-дисплей, розроблений китайською компанією BOE, який може ховатися всередину корпусу і виходити з нього. Це дозволяє змінювати площу дисплею, не складаючи смартфон.

Звичайно, додавання механічної складності пристрою, який буде бовтатися в сумках і час від часу падати, створює певні проблеми. Інженери напевно спробують зробити його якомога більш довговічним і надійним. Це особливо важливо, якщо врахувати той факт, що, на відміну від складних, скручують телефони ще не пройшли перевірку масовим користувачем.

Як повідомляє Nikkei Aisia, унікальний смартфон LG Rollable з розсувним екраном - не просто концепт. Офіційний представник LG підтвердив, що LG Rollable надійде в продаж в кінці цього року. TCL також демонструвала прототип смартфона з висувним екраном на початку 2020 року, хоча зазначила, що таке пристрій не комерційно доступно протягом деякого часу, оскільки механізм все ще потребує вдосконалення. З огляду на швидкість, з якою Oppo і TCL зазвичай працюють над концептами смартфонів, можна допустити, що в 2021 році ми отримаємо два або три конкуруючих апарату зі скручується дисплеями.

Література:

1. https://mind.ua/ru/publications/20220850-ces-2021-10-vau-novinok-glavnoj-vystavki-elektroniki

2. https://www.ixbt.com/news/2021/01/13/unikalnyj-smartfon-lg-rollable-s-razdvizhnym-jekranom--ne-prosto-koncept-on-vyhodit-v-jetom-godu.html

3. https://3dnews.ru/1029748/lg-pokazala-razdvignoy-smartfon-rollable-so-skruchivaemim-displeem

THE INTERNET OF BODIES IS HERE. WHAT SHOULD WE EXPECT?

Leliovska Diana
Institute of Information Technologies
State University of Telecommunications
Kyiv

We're entering the era of the "Internet of Bodies": collecting our physical data via a range of devices that can be implanted, swallowed or worn. The result is a huge amount of health-related data that could improve human wellbeing around the world, and prove crucial in fighting the COVID-19 pandemic.

But a number of risks and challenges must be addressed to realize the potential of this technology, from privacy issues to practical hurdles.

The Internet of Bodies or IoB, the imminent development in the widespread Internet of Things(IoT) domain, is the unavoidable future of technology right now. In simple terms, IoB is IoT entering the human body. Instead of devices connected to the internet as in IoT, it's human bodies that are now connected to a network, with the potential to be remotely controlled and monitored. In short, our bodies will become the new data discovery platform. Internet of Bodies is referred to as the future of tech, but this future isn't that far away. At present, IoB, a form of embodied intelligence, has found its presence in the health care domain. Pacemakers for heart patients is the most common example.

There are three generations of Internet of Bodies that include:

- Body external: These are wearable devices such as Apple Watches or Fitbits that can monitor our health.
- Body internal: These include pacemakers, cochlear implants, and digital pills that go inside our bodies to monitor or control various aspects of our health.
- Body embedded: The third generation of the Internet of Bodies is embedded technology where technology and the human body are melded together and have a real-time connection to a remote machine.

A recent instance of body-embedded systems involves Three Square Market, a Michigan based company that develops micro-market break room solutions for vending operators. A recent CNBC report says that 50 out of their 80 employees agreed to have a radio frequency identification (RFID) microchip, which is the size of a grain, implanted under their skin. The function of the chip is to make identification possible with just a wave of hand, eliminating the need for biometric identification methods, having to carry an identity card, or even remembering a password. Your presence anywhere in the premises could be detected. Now that will be the forerunner of the cyborgs that we hope to see anytime soon. However, the concept of chipped employees in fact poses the problem of consent from the side of employees and is a big intrusion into the privacy of the people involved. It is actually quite difficult to believe that the aforementioned employees willingly let the chips to be implanted on them.

In the special wards of Shanghai's Public Health Clinical Center, nurses use smart thermometers to check the temperatures of COVID-19 patients. Each person's temperature is recorded with a sensor, reducing the risk of infection through contact, and the data is sent to an observation dashboard. An abnormal result triggers an alert

to medical staff, who can then intervene promptly. The gathered data also allows medics to analyse trends over time.

The smart thermometers are designed by VivaLNK, a Silicon-Valley based startup, and are a powerful example of the many digital products and services that are revolutionizing healthcare. After the Internet of Things, which transformed the way we live, travel and work by connecting everyday objects to the Internet, it's now time for the Internet of Bodies. This means collecting our physical data via devices that can be implanted, swallowed or simply worn, generating huge amounts of health-related information.

But there are some challenges faced by Internet of Bodies Technology. The situation of U.S. Vice President Cheney getting a defibrillator not connected to WiFi for security reasons illustrates one of the biggest challenges faced by Internet of Bodies technology—how to secure the devices and information they collect and transmit. Nearly half a million pacemakers were recalled in 2017 by the U.S. Food and Drug Administration over security issues requiring a firmware update. The security challenges faced by Internet of Bodies tech are similar to what plagues Internet of Things generally, but there can be life and death consequences when IoB devices are involved. Additionally, IoB devices create another cyber security challenge that will need to be safeguarded from hackers.

Privacy is also of paramount concern. Questions about who can access the data and for what purpose need answers. For example, a device that monitors health diagnostics could also track unhealthy behaviors. Will health insurance companies be able to deny coverage when a customer's IoB device reports their behavior? A cochlear implant could restore hearing, but it might also record all audio in a person's environment. Will that data remain private?

As Internet of Bodies tech continues to grow, regulatory, legal issues will have to be resolved, and policies built around the proper use of the technology.

References:

1. https://medium.com/ieeekerala/internet-of-bodies-an-overview-9302579af62c

2. https://www.weforum.org/agenda/2020/06/internet-of-bodies-covid19-recovery-governance-health-data/

3. https://www.forbes.com/sites/bernardmarr/2019/12/06/what-is-the-internet-of-bodies-and-how-is-it-changing-our-world/?sh=1d0fb82468b7

КЛАСИФІКАЦІЯ РОБОТИЗОВАНИХ ТЕХНОЛОГІЧНИХ КОМПЛЕКСІВ

Лєнська Ірина Станіславівна

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Характерною рисою сучасної науково-технічної революції є широке впровадження роботів в сферу виробництва і наукових досліджень. Роботи представляють собою універсальні автомати для відтворення рухових та інтелектуальних функцій людини. Одним з важливих класів їх є маніпуляційні роботи. Практичною метою створення роботів є передача їм тих видів діяльності, які для людини трудомісткі, важкі, монотонні, шкідливі для здоров'я і життя. Роботи застосовуються для комплексної автоматизації виробництва, зростання продуктивності праці, поліпшення якості продукції.

Розвиток сучасної техніки все більше вказує на тісну інтеграцію апаратних і програмних частин пристроїв, яка виливається в інтегральні системи, звані "Мехатронні". Мехатроніка є молодою областю науки і техніки, яка виділилася в самостійний напрям зовсім недавно. Термін складається з двох частин - "меха", від слова механіка і "троніка", від слова електроніка. В широкому розумінні цього слова мається на увазі злиття трьох областей наук:

1) електроніки, що включає мікроелектроніку, силову електроніку, перетворювачі і вимірювачі інформації;

2) механіки і електромеханіки, що включають механічні елементи, машини, приводи, точну механіку і електричний елементи;

3) інформаційні технології, що включають теорію систем, моделювання, програмне забезпечення, штучний інтелект.

Одна з причин пильної уваги до мехатроніки в даний час - постійне підвищення вимог до автоматизації виробництва і пов'язана з цим необхідність створення виробничих машин і комплексів з них - механічних систем з принципово новими властивостями.

Маніпуляційний робот являє собою багатоступеневий, багатофункціональний маніпулятор, призначений для того, щоб відтворювати деякі робочі функції людських рук з метою виконання різних робіт [1].

За своєю структурою маніпулятор - багатоланкова машина, між окремими елементами якої існують механічні зв'язку. Залежно від галузі застосування можуть використовуватися різні схеми побудови механічної частини маніпулятора, але все ж основна конструкція являє собою послідовність ланок, з'єднаних між собою обертовими/поступальними парами [2]. Більшість вироблених в даний час маніпуляторів відносяться до числа роботів з обертальною системою координат. Вони забезпечують найбільший обсяг робочої зони, в якій може здійснюватися рух. Їх структура дозволяє досягати заданого положення і орієнтації робочого органу, в тому числі при накладенні обмежень на

можливі переміщення, що виникають при наявності перешкод в робочій зоні.

З боку механіки маніпулятор є системою твердих, пружних тіл, які пов'язані з допомогою різних видів зв'язків. З боку теорії механізмів будь-якої розглянутий маніпулятор є системою декількох тіл, які призначені для того щоб перетворювати переміщення тіл в потрібні переміщення відмінних від них тіл, що говорить про те, що маніпулятор є просторовим механізмом з потрібним для функціонування числом ступенів свободи. Тіла, є твердими і входять в механічну систему маніпулятора, названі ланками. Дві дотичні один з одним ланки, що знаходяться в рухомому з'єднанні, називаються кінематичної парою. Классіфікація кінематичних пар може бути, як за кількістю зв'язків, так і за кількістю ступенів свободи органів механізму [3]. З'єднання ланок, які утворюють між собою кінематичні пари, класифікується як кінематична ланцюг.

Число ступенів будь-якого розглянутого механізму визначається числом узагальнених координат, за які приймаються деякі незалежні змінні, які можуть однозначно визначити положення маніпулятора в просторі. Основними виробниками маніпуляційних роботів є фірми KUKA, Fanuc, Yaskawa.

Відзначимо, що випускаються в даний час маніпулятори, в більшості своїй, мають шістьма і більш ступенями свободи, так як це дозволяє забезпечити більш зручне і точне позиціонування і орієнтацію робочого органу в просторі

Література:

1. Борисов О.И., Громов В.С., Пыркин А.А., Методы управления робототехническими приложениями. Учебное пособие. — СПб.: Университет ИТМО, 2018. — 108 с.

2. Hartley R., Zisserman A. Multiple View Geometry in Computer Vision // Cambridge University Press, 2017.

3. С.Ф. Бурдаков А., В.А. Дьяченко. Проектирование манипуляторов промышленных роботов и роботизированных комплексов. М.: Высшая школа, 2015. – 264 с

ВІРТУАЛЬНА РЕАЛЬНІСТЬ

Лобода Юрій В'ячеславович
Навчально-науковий інститут Інформаційних технологій
Державний університет телекомунікацій
м. Київ

Як влаштована віртуальна реальність і як в неї потрапити? Якщо бути точним - то за рахунок деякого впливу на органи чуття та надання сигналу на них. Майже все населення вже знає, що в світі існує така річ, як "віртуальна реальність", але більше детально розглянувши цей світ, можна дивитись на всю

комп'ютерну техніку зовсім по-іншому. Тож, спробуємо дізнатись, що це таке і з чим його їдять.

Віртуальна реальність - технологічно реалізований світ, який людина сприймає через відчуття, перш за все, зір і слух. Прогресивні технології за допомогою спеціального обладнання і високоякісної комп'ютерної графіки готові зробити достовірну реальність, в яку зможе зануритися будь-хто.

Так як більшу частину інформації людина сприймає через зір, саме зорова основоположна вважається найважливішою і характеризуючою при розробці близького до реальності занурення. Дана інформація також багато в чому характеризує наше почуття простору і рівноваги - ось тому в віртуальній реальності неважко відчути запаморочення. За візуальну частину відповідають екрани з високою роздільною здатністю і калібруючими лінзами або ретинальні проектори, які виводять зображення саме на сітківку.

Багатоканальний звук, відтворюваний через навушники - також не менш важлива частина, що робить реалістичне відчуття оточення. Зручним чином 2 вищезгадані системи поєднуються в шоломах віртуальної реальності - найбільш популярним пристроєм для VR-розваг. Шоломи віртуальної реальності забезпечені особливими контролерами, що зчитують положення рук гравця, для забезпечення його взаємодії зі світом. Крім цих завдань, як переміщення і вплив на внутрішньоігрові об'єкти, контролери можуть передавати і зворотній взаємозв'язок, наприклад, вібруючи, при отриманні пошкоджень.

Тож, як грати в віртуальній реальності? Для початку, купимо шолом. Найбільш популярним на ринку, на сьогоднішній день, являється виробник Oculus Rift. Вони дають якісне занурення в реальність.

Друга річ, яка потрібна для того, щоб грати в ігри в віртуальній реальності - це, звичайно ж, ігри. Ігри, які підтримують VR можна розділити на дві категорії: класичні ігри з доповненням реальності і ігри, які розроблені спецільно для віртуальної реальності. І, хоча, віртуальна реальність має можливість варіювати враження від проходження класичних ігор, часто їх геймплей спочатку не розрахований на таку можливість, в зв'язку з чим, управління може бути незручним і неприємним. В той момент, ігри 2-ої категорії припускають VR як обов'язкову частину власного ігрового процесу, набагато краще оптимізовані і дають воістину неповторний ігрову навичку.

Ще одна річ, яку потрібно знати всім, хто бажає відчути на собі всі переваги світу віртуальної реальності - це, звичайно ж,

застереження, щоб нікому не нашкодити, в першу чергу, собі. Ці технології практично не мають протипоказань. Варто звернути увагу на своє самопочуття, підбираючи віртуальну розвагу. Так, гра в просторі віртуальної реальності протипоказана вагітним, людям з хворобами серцево-судинної системи, маленьким дітям. І ще небажано прибувати в VR- клуб в стані алкогольного або наркотичного сп'яніння. Так як це може бути небезпечно як для самого гравця, але і для оточуючих.

Література:
1. *https://uk.wikipedia.org/wiki/Віртуальна_реальність*
2. *https://www.it.ua/knowledge-base/technology-innovation/virtualnaja-realnost-vr*

ХМАРНІ СХОВИЩА ДАНИХ

Лобода Юрій В'ячеславович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Щодня люди і компанії генерують гігантську кількість контенту. Якби не хмарні технології, майже все знадобилося б безповоротно видаляти. Розглянемо більш детальніше що таке "хмарні сховища даних", а також які бувають хмарні сховища і де їз частіше всього використовують.

Хмарне сховище - це засіб зберігання і отримання будь-яких даних, що знаходяться в довільній частині інтернету і доступні в будь-якій точці глобальної мережі.

Причин для розміщення даних в хмарному сховищі може бути досить чимало, і для різних користувачів вони можуть мати свої пріоритети.

Наприклад, для приватних осіб більш значуща буде можливість доступу до даних з різних місць інтернету і з різних пристроїв, а для корпоративних користувачів найбільш істотними можуть виявитися надійність і вартість зберігання.

Це не вичерпний перелік тем для застосування хмарного сховища. Наприклад, для корпоративних користувачів може також мати величезне значення.

Тож, давате з'ясуємо, які ж хмарні сховища можуть нам трапитись.

Розташовувати в інтернеті можна різні дані, різноманітно організовані, тому і сховища також можуть бути різними. Хоча, щоб перейти до розгляду типів інтернет-сховищ, потрібно зробити 1 застереження: дані в них можуть зберігати не тільки користувачі, але і додатки, якими, до того ж, користуються люди або фірми. Наприклад, багато програм для зв'язку - Skype,

WhatsApp, Facebook Messenger та інші - зберігають контакти користувачів у власних інтернет-сховищах.

З точки зору користувача, інтернет-сховище має можливість виглядати як допоміжний локальний диск або папка для розміщення довільних файлів. Заключний варіант відмінно знайомий численним користувачам сервісів Dropbox, OneDrive, Google.Drive.

На даний момент, нерідко хмарними дисками називають сервіси виду Dropbox, OneDrive, що некоректно. Дані ресурси надаються користувачам або через веб-інтерфейс, або у вигляді папок на робочому столі. У двох випадках мова не може йти про диски. Наприклад, їх неможливо відформатувати в відповідну файлову систему.

Хоча, дисковий простір сховища дійсно може бути представлено якомусь користувачу через інтернет так, щоб воно приймалося як локальний диск, з яким будуть доступні всі дискові операції.

Для надання дискового простору через інтернет є особливі протоколи, наприклад, Internet Small Computer Systems Interface (iSCSI), iFCP (Internet Fibre Channel Protocol) або Fibre Channel over IP (FCIP). На їх базі робляться, так звані, мережі зберігання даних (SAN, Storage Area Network). За даними протоколів дискові пристрої представляються серверу, до якого вони підключаються, на самому низькому - блоковому - рівні, і тому, вважаються універсальними.

Література:
1. *https://uk.wikipedia.org/wiki/Хмарні_сховища*
2. *https://aws.amazon.com/ru/what-is-cloud-storage/*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Локойда Андрій Олегович, Май Павло, Левін Микола Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Технології сьогодні розвиваються такими швидкими темпами, дозволяючи прискорювати зміни і прогрес, викликаючи прискорення темпів змін, поки в кінцевому підсумку вони не стануть експоненціальними. Однак еволюціонують не тільки технологічні тренди і топові технології, в цьому році багато що змінилося через спалах COVID-19, що змусило IT-фахівців усвідомити, що їх роль завтра не залишиться колишньою в безконтактному світі. А IT-фахівець в 2021 році буде постійно вчитися, розучуватися і переучуватися.

Введення

Щороку в цій галузі виникають нові тенденції, і професіоналам стає важливо бути знайомими з цими різними тенденціями і всім, що вони тягнуть за собою. Незалежно від того, в якій професії Ви працюєте, знайомство з ними може поліпшити ваш професійний статус і допомогти вам зрозуміти, які потенційні поліпшення для галузі, в якій ви вже працюєте. Ось топ-6 нових технологічних трендів, які ви повинні спостерігати і спробувати реалізувати в 2021 році, і, можливо, забезпечити собі одне з робочих місць, які будуть створені цими новими технологічними трендами. [1, с. 60–61]

1. Штучний інтелект і машинне навчання

Штучний інтелект, який вже отримав багато шуму в останнє десятиліття, але він продовжує залишатися одним з нових технологічних трендів, оскільки його помітний вплив на те, як ми живемо, працюємо і граємо, знаходиться тільки на ранніх стадіях. Штучний інтелект вже відомий своєю перевагою в розпізнаванні зображень і мови, навігаційних додатках, персональних помічниках смартфонів, додатках для обміну поїздками і багато іншого. Крім того, штучний інтелект буде використовуватися надалі для аналізу взаємодій, визначення лежать в їх основі зв'язків та ідей, для прогнозування попиту на такі послуги, як лікарні, що дозволяють владі приймати більш ефективні рішення про використання ресурсів, а також для виявлення мінливих моделей поведінки клієнтів шляхом аналізу даних майже в режимі реального часу, підвищення доходів і поліпшення персоналізованого досвіду. Ринок штучного інтелекту зросте до 190 мільярдів доларів до 2025 року, а глобальні витрати на когнітивні системи та системи штучного інтелекту досягнуть понад 57 мільярдів доларів у 2021 році. [1, с. 73–78]

2. Роботизована Автоматизація технологічних процесів

Подібно до штучного інтелекту та машинного навчання, роботизована автоматизація процесів - це ще одна технологія, яка автоматизує робочі місця. Робототехнічна автоматизація процесів-це використання програмного забезпечення для автоматизації бізнес-процесів, таких як інтерпретація додатків, обробка транзакцій, робота з даними та навіть відповіді на електронні листи. Роботизована автоматизація процесів автоматизує повторювані завдання, які раніше виконували люди. Роботизована автоматизація процесів також створює нові робочі місця, змінюючи існуючі. McKinsey вважає, що менше 5% професій можуть бути повністю автоматизовані, але близько 60% можуть бути частково автоматизовані. [2, с. 52–54]

3. Граничні обчислення

Останнім часом хмарні обчислення стали популярними, а великі гравці Amazon Web Services, Microsoft Azure і Google Cloud Platform домінують на ринку. Впровадження хмарних обчислень все ще зростає, оскільки все більше і більше компаній переходять на хмарні рішення. Оскільки кількість даних, з якими стикаються організації, продовжує зростати, вони усвідомили недоліки хмарних обчислень в деяких ситуаціях. Граничні обчислення покликані допомогти вирішити деякі з цих проблем, щоб обійти затримку, викликану хмарними обчисленнями, і доставити дані в центр обробки даних для обробки. У деяких ситуаціях граничні обчислення можуть діяти як міні-центри обробки даних. Прикордонні обчислення будуть збільшуватися в міру збільшення використання пристроїв Інтернету речей (IoT). Очікується, що до 2022 року світовий ринок граничних обчислень досягне 6,72 мільярда доларів. І ця нова технологічна тенденція покликана тільки зростати і ні більше ні менше, створюючи різні робочі місця, в першу чергу для інженерів-програмістів. [1, с. 80–84]

4. Квантові обчислення

Наступним технологічним трендом є квантова обчислювальна техніка, яка використовує переваги квантових явищ, таких як суперпозиція і квантова заплутаність. Ця технологічна тенденція також бере участь у розробці потенційних вакцин, завдяки своїй здатності легко запитувати, відстежувати, аналізувати та діяти на основі даних, незалежно від джерела. Ще одна область, де квантові обчислення знаходять застосування, - це банківська справа і фінанси, управління кредитним ризиком, високочастотна торгівля і виявлення шахрайства. Квантові комп'ютери в даний час набагато швидше, ніж звичайні комп'ютери, і великі бренди, такі як Splunk, Honeywell, Microsoft, AWS, Google та багато інших, зараз беруть участь у створенні інновацій квантових обчислень. За прогнозами, до 2029 року виручка світового ринку квантових обчислень перевищить 2,5 мільярда доларів. І щоб зробити помітний крок у цій новій технології, ви повинні мати досвід роботи з квантовою механікою, лінійною алгеброю, ймовірністю, теорією інформації та машинним навчанням. [3, с. 86–88]

5. Віртуальна реальність та доповнена реальність

Наступна технологічна тенденція - віртуальна реальність (VR) та доповнена реальність (AR) та розширена реальність (ER). VR занурює користувача в середовище, тоді як AR покращує його середовище. Хоча ця технологічна тенденція до

цього часу в основному використовувалась для ігор, вона також використовувалась для тренувань, як і у VirtualShip, імітаційному програмному забезпеченні, що використовується для навчання капітанів кораблів ВМС США, армії та берегової охорони.

У 2021 році ми можемо очікувати, що ці форми технологій будуть далі інтегровані в наше життя. Зазвичай працюючи в парі з деякими іншими новими технологіями AR та VR мають величезний потенціал у навчанні, розвагах, освіті, маркетингу та навіть реабілітації після травми. Будь-який з них може бути використаний для навчання лікарів хірургічному втручанню, пропонування відвідувачам музеїв глибшого досвіду, розширення тематичних парків або навіть покращення маркетингу, як у цьому притулку для автобусів Pepsi Max. Цікавий факт: у 2019 році було продано 14 мільйонів AR та VR-пристроїв. До 2022 року очікується, що світовий ринок AR та VR зросте до 209,2 мільярда доларів, лише створивши більше можливостей у сучасній технології та запросивши більше професіоналів. Для початку роботи у віртуальній реальності не потрібно багато спеціалізованих знань - базові навички програмування та перспективне мислення можуть дати роботу. [4, с. 40–44]

6. Блокчейн

Хоча більшість людей думає про технологію блокчейну стосовно таких криптовалют, як біткойн, блокчейн пропонує безпеку, яка корисна багатьма іншими способами. Найпростішими словами, блокчейн можна охарактеризувати як дані, до яких ви можете лише додавати, а не вилучати або змінювати. Звідси випливає термін "ланцюжок", оскільки ви створюєте ланцюжок даних. Неможливість змінити попередні блоки - це те, що робить його таким безпечним. Крім того, блокчейни керуються консенсусом, тому жодна сутність не може взяти під контроль дані. З блокчейном вам не потрібна довірена третя сторона для нагляду чи перевірки транзакцій. Кілька галузей залучають та впроваджують блокчейн, і оскільки використання технології блокчейн зростає, зростає і попит на кваліфікованих фахівців. З точки зору пташиного польоту, розробник блокчейну спеціалізується на розробці та впровадженні архітектури та рішень із використанням технології блокчейн. Середньорічна зарплата розробника блокчейну становить 469 тис євро. Щоб потрапити в Blockchain, вам потрібно мати практичний досвід роботи з мовами програмування, основами OOPS, плоскими та реляційними

базами даних, структурами даних, розробкою веб-додатків та мережею. [4, с. 46–48]

Література:

1. Беріша-Шакірі, А., Інформаційні технології та менеджмент, академічний журнал бізнесу, адміністрування, права та соціальних наук; Том l, № 1, березень 2015 р., ISSN 2410-3918, Видавництво "IPCCL", 2015 рік.

2. ГУДАНОВСКАЯ А. Е., Сучасні напрямки досліджень в області технологічного менеджменту в світлі обраних публікацій. Видавництво "Наука", 2017 рік.

3. ЛУКАС, Х.С. Інформаційні технології для управління: глобальний текст, ліцензія CreativeCommons Attribution 3.0, Швейцарія, 2009 рік.

4. ДОЛІНСЕК С. і СТРУКЕЛЬ П., Технологія, багатство і сучасне управління технологіями, управління глобальними переходами, Видавництво "Приморський університет" Словенія, 2012 рік.

ПРО НЕБЕЗПЕКУ МІКРОХВИЛЬОВОГО ВИПРОМІНЮВАННЯ

Луппа Олексій Андрійович, Матвійчук Артем Миколайович, Руденко Віталій Дмитрович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

У багатьох країнах по всьому світу люди збираються в групи для боротьби з новими стандартами зв'язку (наприклад з вишками 5G), багато хто боїться домашнього Wi-Fi, адже, на їхню думку, вони шкодять здоров'ю. Вчені вже давно зацікавилися цією темою та провели низку досліджень у цій сфері.

Коли на початку XX століття Марія Кюрі відкрила новий спосіб добувати радій з настурану, його почали позиціонувати як засіб, який допомагає залишатися здоровим. Тоді навіть почали випускали різноманітні продукти, які містили цей радіоактивний елемент [1]. Ще з 1915 року люди почали говорити про небезпеку електромагнітного випромінювання. Тож не можна вважати, що ця течія у суспільстві нова.

Одним із аргументів сьогодні є збільшення випадків діагностування раку у людей і виникнення патологій у дітей з народження. Їх можна спростувати ще до обговорення електромагнітних хвиль. Рак у людей діагностується частіше насамперед тому, що з розвитком медицини лікарі стали краще його виявляти та лікувати. З патологіями у дітей схожа ситуація: лікарі можуть одразу їх виявляти і ставити діагноз, таких дітей у сучасному світі не ховають вдома, а навпаки, намагаються адаптувати до нормального життя. Тим паче, при гострій необхідності дороговартісної операції, такі випадки широко тиражуються в ЗМІ, що створює відчуття масовості.

Щодо шкоди власне електромагнітних хвиль, вченими точно доведена небезпека випромінювання з частотою вище $3*10^{15}$ Гц, тобто вище частоти видимого світла (наприклад рентгенівське або гамма-випромінювання). Такі хвилі мають велику енергію, тому їх взаємодія з живими організмами може призвести до незворотних пошкоджень у живому організмі.

Сучасні пристрої використовують мікрохвильовий, або навіть менш частотний, діапазон електромагнітного випромінювання для передачі інформації ($3\cdot10^9$–$3\cdot10^{10}$ Гц), який має приблизно від десяти до ста тисяч раз меншу енергію в порівнянні з тими, що точно наносять шкоду живим організмам.

ВОЗ зазначає, що при проведенні власного десятилітнього дослідження на тему негативного впливу мобільних телефонів на організм людини не було встановлено жодних негативних наслідків для здоров'я, спричинених використанням мобільних телефонів [2].

Також у доповіді ВОЗ зазначено, що основним механізмом взаємодії радіочастотного випромінювання з людським тілом є його нагрівання, тобто воно за своєю суттю не спричиняє онкологічні відхилення в людському організмі.

Щодо небезпеки Wi-Fi дослідження проводила Англійська асоціація по охороні здоров'я. Їхнє дослідження також не виявило негативного впливу на людину, адже потужність сигналу від роутера приблизно дорівнює 0.1 Ват, що в рази менше ніж від мобільного телефону від час розмови [3].

Також, на інформаційній інтернет платформі «EMF-Portal» Рейнсько-Вестфальського технічного університету Аахена опубліковане дослідження про вплив ЗМІ на самонавіювання людей. Так, одній групі людей показали короткий фільм про небезпеку бездротових мереж, а потім сказали їм, щоб увімкнули Wi-Fi у кімнаті. Невдовзі більшість піддослідних почала відчувати симптоми, описані у фільмі. Проблема в тому, що жодного Wi-Fi у кімнаті не вмикалося [4].

Отже, на сьогоднішній день не доведено жодного негативного впливу мікрохвильового випромінювання від мобільних телефонів або Wi-Fi. Проте ВОЗ у 2013 році занесла таке випромінювання у групу 2В списку канцерогенних факторів для людини [5] як можливо небезпечне, без доведеного негативного впливу.

Література:

1. https://www.mentalfloss.com/article/12732/9-ways-people-used-radium-we-understood-risks

2. https://www.who.int/en/news-room/fact-sheets/detail/electromagnetic-fields-and-public-health-mobile-phones

3. https://webarchive.nationalarchives.gov.uk/20140714065433/http://www.hpa.org.uk/webw/HPAweb&Page&HPAwebAutoListName/Page/1199451940308
4. https://www.emf-portal.org/en/article/21586
5. https://monographs.iarc.fr/list-of-classifications

СУЧАСНІ ХМАРНІ ТЕХНОЛОГІЇ ТА ТЕХНОЛОГІЇ ВЕЛИКИХ ДАНИХ

Луппа Олексій Андрійович
Матвійчук Артем Миколайович
Руденко Віталій Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут
інформаційних технологій
м. Київ

Хмарні технології займають все більш загальноприйняту позицію серед платформ для побудови додатків для веб, бізнесу, промисловості та сучасних наукових досліджень. Саме вони надають додаткам такі якості, як виділення ресурсів і надання послуг за вимогами, горизонтальна і вертикальна масштабованість, мобільність, незалежність від програмної та апаратної платформ.

Хмарні технології – це здатність системи до розподіленої обробки цифрових даних, за допомогою чого комп'ютерному користувачеві надаються ресурси для потрібних операцій. Досить важкі програми мають можливість запускатись та виконуватись у вікні браузера ПК, а усі програми знаходяться на віддаленому сервері та тільки кешуються на комп'ютері користувача.

Основна перевага цієї технології заключається в тому, що користувач має доступ до всіх потрібних даних, але не піклується про інфраструктуру, операційну систему та програмне забезпечення. [1]

Взагалі, хмарне середовище зберігання даних – це модель сховища, в якому уся інформація клієнта розподілена по різним серверам. Таким чином користувач отримує велику кількість пам'яті для зберігання даних, не купуючи окремі носії. [3]

Існують три рівні хмарних технологій:

1. Перший та найнижчий рівень – це надання користувачам прав на використання певного програмного забезпечення. Таким чином користувачі отримують потужну машину, яка має у собі певне програмне забезпечення, що надає можливість працювати над потрібним проектом не задумуючись о архітектурі системи.

2. Другий рівень надає можливість отримати в своє розпорядження операційні системи, системи управління базами

даних або засоби розробки і налагодження. Це робить створення ПО та розробку інших проектів ще більш гнучким процесом.

3. Третій рівень віддає користувачеві всю мережеву інфраструктуру, яка може бути корисною для розгортання великих проектів з різними сервісами та можливостями.

Хмарні технології мають великий потенціал, основними перевагами є те, що вони надають доступ до будь-яких можливостей, не спираючись на характеристики системи користувача. Вони можуть бути використані у любій точці світу для будь-яких цілей.

А от основними недоліками цих технологій є безпека та стабільність інтернету, яка повина бути на високому рівні для комфортної роботи усіх сервісів. Ніхто не можете гарантувати збереження ваших даних та ви надаєте усю інформацію компанії, яка надає вам хмарні технології.

Література:

1. *https://edin.ua/shho-take-xmarni-texnologi%D1%97-i-navishho-voni-potribni/*
2. *https://en.wikipedia.org/wiki/Cloud_computing*
3. *https://maylohack.ru/uk/ios/harakteristika-oblachnyh-uslug-oblachnye-tehnologii-chto-takoe.html*

СИСТЕМИ ВІДЕОНАГЛЯДУ НА БАЗІ ХМАРНИХ ТЕХНОЛОГІЙ

Ляшенко Владислав Віталійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У даній статті розглядається питання особливостей застосування систем відеонагляду у сучасному світі. Системи відеонагляду на базі хмарних технологій знаходять широке застосування в областях, де традиційні аналогові системи відеонагляду не можуть бути застосовані. Наприклад, для розв'язання проблем, де необхідно, щоб був віддаленний доступ до системи відеонагляду для того щоб виконувати моніторинг у реальному часі знаходячись у будь-якій точці світу.

У статті розглянуться шляхи застосування систем відеонагляду на базі хмарних технологій та порівняння з аналоговими системами відеонагляду.

Вступ

У наш час відеоспостереження стало невід'ємною частиною комплексної системи безпеки, тому що нинішні системи відеоспостереження можуть не тільки показувати і записувати відео, але і програмувати реакцію всієї системи безпеки в разі нештатних ситуацій. Залежно від типу оснащення системи відеоспостереження поділяють на аналогові і цифрові. Аналогові системи відеоспостереження застосовуються, де потрібно зробити систему відеоспостереження в маленькій

будівлі і зображення з камер записувати на відеомагнітофон. Цифрові системи відеоспостереження, роз'єднуються в розподілені системи безпеки. Такі комплекси, записують і розглядають інформацію, що надходить від камер, а також "приймають рішення" щодо збереження охороняється об'єкта в оффлайн режимі або по підтвердженню оператора системи. Цифрова система відеоспостереження застосовується в системах безпеки територіально поділених об'єктів. Сьогодні цифрові системи відеоспостереження мало-помалу виштовхують з ринку аналогові системи по функціональних і технічних якостях, а так само за своєю вартістю вже наближаються до вартості аналогових систем відеоспостереження. Здібності, характеристики та збирання системи відеоспостереження залежать від вимог замовника. Як правило, невеликий склад такої системи включає в себе, пристрої обробки відеосигналів, записуючий пристрій (відеомагнітофони, відеореєстратори, відеорекордери) (квадратори, мультиплексори і ін.), Відеокамери, і пристрої опису відеоінформації (відеомонітори). У великі системи відеоспостереження монтують додаткові керуючі і допоміжні пристрої - клавіатури управління відеокамери, модулятори, матричні комутатори, підсилювачі-розподільники, Відеопринтери, телеметричні приймачі і датчики та інші охоронні пристрої.

Основна частина

Як правило, в будь-яку сучасну систему відеоспостереження входять не тільки традиційні відеокамера і телевізор для перегляду інформації, що передається з неї зображення, сьогодні система відеоспостереження являє собою справжнісіньку мережу елементів, з'єднаних один з одним за допомогою передачі сигналів за допомогою радіохвиль або кабелю. Залежно від того, які саме прилади входять в систему відеоспостереження, розрізняють системи декількох основних типів. Охоронні системи відеоспостереження умовно можна розділити на два види: провідні і бездротові. Яку саме систему застосовувати на об'єкті залежить від його особливостей (величина території, що охороняється, наявність пропускної системи входу, пр.).

Крім даної класифікації, системи відеоспостереження поділяють на цифрові і аналогові. Безумовно, цифрове відеоспостереження за багатьма показниками перевершує аналогову систему. Однак і вартість комплекту цифрової системи також має серйозні відмінності.

Аналогові системи відеоспостереження. У минулому

столітті установка відеоспостереження була побудована на аналогових камерах, мікшерах і моніторах, сучасне охоронне відеоспостереження витісняє старі системи і в багатьох комплексах практично не використовує аналогові системи, майже повністю переключившись на цифровий формат [1, с.17-20].

Тенденція розвитку цифрових технологій ніколи не зможе повністю витіснити аналогову апаратуру, так само, як цифрова фотографія не замінить фотодрук. Звичайно, передача аналогових сигналів неефективна, низька завадостійкість, втрата сигналу, складність в записі і обробці цифрових сигналів. Проте, охоронне відеоспостереження не виключає можливості використання аналогових камер. Установка відеоспостереження на основі аналогових відеокамер не втрачає своєї популярності. Серед безлічі недоліків аналогового відеоспостереження, є суттєві позитивні сторони.

В основі кожної подібної системи лежить аналогова відеокамера, об'єднана в мережу з відеореєстраторами, мультиплікаторами, спеціальними пристроями для зберігання інформації і її виведення. Аналоговий сигнал з відеокамери надходить безпосередньо на відеореєстратор, дозволяє налаштовувати необхідні режими управління системою, запис і виведення необхідної інформації на монітори і ін. Мультиплікатор в даній мережі використовується для того, щоб мати можливість в один і той же час отримувати і обробляти сигнали з декількох відеокамер , завдяки чому структура мережі в цілому значно спрощується. У випадку з аналоговими системами відеоспостереження вся отримана інформація зберігається на магнітних носіях. Недоліком аналогової системи є велика кількість взаємодіючих між собою приладів, через що такий варіант вважається досить громіздким для реалізації, і навряд чи може зрівнятися з цифровими або змішаними системами, про які піде мова далі. Система складається з наступних елементів: відеокамера, вона є очима системи. Відеокамера перетворює світловий потік в електричний сигнал, величина якого пропорційна інтенсивності світлового потоку. Далі, дані від відеокамери можуть передаватися до наступних пристроїв як по проводах, (коаксіальний кабель, вита пара, оптоволокно), так і по системам радіозв'язку, як правило, працюють в гігагерцовий діапазоні.

В аналогових системах, щоб ефективно управляти камерами, застосовуються такі пристрої, як перемикачі (квадратори), мультиплексори і матричні системи.

Перемикач (квадратор) - це пристрій, що має кілька

входів для відеокамер і дозволяє оператору довільно переключати виведене на монітор або записується зображення з будь-якої камери, або включати послідовне автоматичне перемикання камер. Можливості таких пристроїв обмежені, тому їх застосування доцільно лише в найпростіших системах.

Мультиплексор є більш «просунутим» пристроєм. Він дозволяє виводити на один монітор кілька камер і вести одночасний запис з декількох джерел відеосигналу. На відміну від квадратора мультиплексор може містити в собі детектор руху і має більше можливостей управління камерами.

Матричні системи - наступний рівень розвитку мультиплексорів. Вони призначені для обслуговування великих підприємств, де встановлено велику кількість камер і є кілька операторів.

Монітор для відеоспостереження відрізняється від звичайного телевізора більш чітким зображенням і високою роздільною здатністю. Люмінофор, який використовується в таких моніторах, має підвищену стійкість, тому що зображення може багато годин залишатися нерухомим.

Як правило, в системах відеоспостереження використовуються спеціальні пристрої запису, що записують на стандартну відеоплівку, але розраховані на більший час запису, тому що не завжди необхідно плавне зображення з частотою 25 кадрів в секунду. Відеомагнітофони, які найбільш часто застосовуються спільно з системами спостереження, відносяться до класу TLVR. (Відеомагнітофонів з затримкою часу). Такі пристрої дозволяють стандартну тригодинну плівку "розтягнути" при використанні до 960 годин. Швидкість протягання плівки в даному випадку змінюється східчасто (3 години, 12 годин; 24 години; 48 годин, ... 960 годин). Крім того, в таких системах можливий запис зображення одночасно з декількох відеокамер [2, с.17-20].

Переваги аналогових систем відеоспостереження. Встановлення відеоспостереження та його налаштування, набагато простіше, ніж установка відеоспостереження цифрового формату. Це пов'язано з виключенням цифровий синхронізації між камерами і устаткуванням для запису сигналу. Аналогове охоронне спостереження на порядок дешевше, ніж рівносильне цифрове обладнання, тому установка відеоспостереження на аналогових відеокамерах в невеликих магазинах або офісах прийнятно по бюджету і досить ефективна.

Цифрове охоронне відеоспостереження відрізняється від аналогового зручністю зберігання і обробки даних. Відеосервери мають можливість оцифровки сигналу, таким

чином, на аналогових відеосистемах можна організувати якісне охоронне відеоспостереження. За допомогою відеосерверов аналогові камери можна підключати до мереж.

Не дивлячись на складність підвищення дозволів зображення і швидкості, встановлення відеоспостереження на основі аналогових камер користується попитом. Якість передачі кольору для кольорових аналогових камер значно вище, крім того, в порівнянні з цифровим відеоспостереженням аналогові системи краще працюють в темряві, чутливість матриці досить висока, щоб можна було розрізнити не тільки силует, але і особа злочинця. Аналог краще працює в темряві, тому установка відеоспостереження базується не на сучасності того чи іншого обладнання, а на конкретних завданнях позначених для складання проекту.

Багато наших клієнтів, працюють з професійним обладнанням, ведуть охоронне відеоспостереження, і використовують аналогові відеокамери. Ми можемо з упевненістю сказати, що за весь час обслуговування аналогових систем проблем з апаратурою такого класу не виникало.

IP-відеоспостереження на базі хмарних технологій. IP відеоспостереження - один з поширених методів у сучасних системах спостереження та охорони. Всі великі виробники електроніки намагаються зробити свою техніку ip сумісною [1, с. 40-42]. IP - це протокол (InternetProtocol) міжмережевоговзаємодії. Він дозволяє пристроям підключатися до мережі і взаємодіяти за допомогою програм з комп'ютером.

Саме IP відеоспостереження використовується в сучасних системах охорони, нових системах виявлення та аналізу предметів, для автоматичного розпізнавання номерних знаків автомобілів. Монтаж відеоспостереження на основі IP дозволяє об'єднати відеокамери за допомогою існуючої мережі, звернення до камери можливо безпосередньо з комп'ютера, достатньо просто ввести ip адреса камери.

Монтаж відеоспостереження займає мінімум часу, камери швидко встановлюються. IP відеоспостереження підходить як для роботи всередині приміщень, так і зовні. Для вуличного спостереження використовується спеціальний кожух і об'єктив. Камери для ip відеоспостереження мають функцію пре і пост записи (за сигналом тривоги), для цього використовується карта пам'яті [1, с.271-274].

IP відеокамери бувають декількох типів, високочутливі, панорамні, купольні, з високою роздільною здатністю 1280x1024 пікс. і швидкістю до 30 к / с. Всі вони розроблені для організації систем охорони і спостереження. Для ip

відеоспостереження випускаються спеціальні кожухи до камер, для роботи в умовах підвищеної вологості, низьких температур і навіть антивандальний кожух для міського ір відеоспостереження.

Монтаж відеоспостереження з використанням IP, зазвичай здійснюється спільно з організацією локальних мереж. Наша компанія розробляє проекти пов'язані не тільки з IP відеоспостереженням, а й комплексні рішення організації безпеки. Такі як, системи контролю доступу, автоматизовані парковки або АТС телефонія. IP-системи відеоспостереження стали активно входити в повсякденне життя, і на сьогодні ця технологія відеоспостереження вважається останнім досягненням в області охоронних систем контролю об'єктів. Сучасні і неймовірно зручні системи IP спостереження застосовуються повсюдно в самих різних установах і об'єктах - в банках, на вокзалах, школах, медичних установах, адміністративних об'єктах, ресторанах, готелях, аеропортах, вокзалах, магазинах. IP відеоспостереження являє собою систему, побудовану на мережевих відеокамерах і відео сервісом, які не тільки фіксують відеозображення, а й посилають цю інформацію через Інтернет, бездротової та локальної мережі, а зафіксовану інформацію можна переглянути на будь-яких пристроях, що мають доступ в Інтернет.

Головна перевага IP технології полягає в можливості побудови мереж відеомоніторингу, безпеки, контролю та дистанційного керування, що не прив'язуючи до відстані. Системи IP відеоспостереження дуже масштабуються та згинання, вони дають можливість інтелектуального аналізу і негайного доступу до відеоданих. Надалі ці системи надають безмежні можливості в модернізації софта, який використовується з IP системах. Технічні переваги створюють попит на цю продукцію. Найбільш затребуване властивість віддаленого моніторингу та управління системою безпеки на об'єкті практично з будь-якої точки. Якість зображення таких камер дуже високо, а сигнал передається майже миттєво. За допомогою комп'ютера і ПО можна стати володарем повноцінної і функціональної системи відеоспостереження.

Програмне забезпечення до IP відеоспостереження є програмний пакет для IP пристроїв, за допомогою якого можна керувати відеореєстратором, здійснювати запис з пристрою в декількох дозволах, а також використовувати кілька пристроїв для зберігання і архівізації інформація для більш ефективного захисту. Такі програмні пакети підтримують кілька мов і можуть автоматично оновлюватися - Samsung SNS-SF001,

SmartecNetStation 4, AVerMedia NXU8032.

IP камера - це цифровий пристрій, що виробляє не тільки відеозйомку, але і її оцифровку, стиск і передачу інформації по мережі.

Далі ip камері повинен присвоюватися ip-адреса. Завдяки програмному забезпеченню для FTP-сервера, web-сервера або e-mail клієнта, камера буде працювати в ній самостійно. Саме цим і відрізняється ip камера від звичайних камер, які вимагають безпосереднього підключення до ПК через USB порти. Крім цього ip-камери можуть працювати з JAVA-апплетами і призначеними для користувача скриптами [3, с.20-50].

Стиснення відеоінформації в ip камерах може бути як програмним, так і апаратним. Програмна компресія дешевше, але з високою ємності обчислювальних алгоритмів стиснення, вона не така ефективна, особливо якщо існує необхідність переглядати відеодані в online режимі. Тому більшість провідних виробників випускають пристрої з апаратною обробкою. Обчислювальним ядром в ip-камері є центральний процесор. Саме за рахунок нього здійснюються операції з виведення стисненого та оцифрованого відеозображення, а також він відповідає за функціонування вбудованого веб-сервера і програми для управління ip камерами. Флеш-пам'ять оновлює керуючі програми і зберігає HTML сторінки. Відеоінформація з камер може передаватися на спеціальні IP відеореєстратори, де вона зберігається на внутрішніх жорстких дисках. IP відеореєстратори можуть мати функцію інтелектуального детектора руху, записувати інформацію за розкладом, переглядати події, а також мати віддалений доступ, завдяки вбудованому програмному забезпеченню. IP відеореєстратори, представлені в каталозі - Microdigital - MDR-H1402, MDR-H0012E, SAMSUNG SRD-440P No HDD, SRD-440P5G, AVerMedai EH1004H-4NANO, Beward BRVL, Infinity VRF-D1600HSR і інші. До пристроїв IP відеоспостереження також відносяться відеосервери, які призначені для роботи в складі цифрової системи відеоспостереження. Такі пристрої перетворять аналоговий відеосигнал з камер в цифровий формат, потім передають його по мережі або для здійснення запису на носій інформації. Як правило, відеосервери встановлюються при наявній аналогової відеосистеми спостереження, з необхідністю передачі зображення по мережі або її записи на цифровий носій. Багато моделей відеосерверов оснащуються вбудованими детекторами руху, а також входами для підключення інших охоронних датчиків. У деяких передбачена функція відновлення подій, що передують сигналу

тривоги і після нього. IP відеосервер істотно підвищує ефективність системи спостереження і забезпечує надійний захист охоронюваного об'єкта, безперервно зберігаючи отримані відеодані. На сайті в інтернеті ви можете ознайомитися з представленими вашій увазі пристроями IP відеоспостереження, вивчити їх характеристики і можливості, для найбільш оптимального вибору - Microdigital MDR-ivs01, Infinity IPX-100, Smartec STS-IPTX161, HikVision DS-6104HCI-12V, Axis Axis -241S і інші. Існує безліч ситуацій, коли IP відеоспостереження стає найбільш оптимальним вибором для побудови системи контролю і спостереження. Наприклад, відеоспостереження за ретрансляторами мобільного зв'язку, нафтопроводів, маленьких магазинів і автозаправок. Організувати централізоване відеоспостереження іншої схеми, не сильно віддалених об'єктів, крім, як за допомогою пристроїв IP відеоспостереження, досить проблематично.

Висновки

У даній статті було розглянуто шляхи застосування систем відеонагляду на базі хмарних технологій та порівняння з аналоговими системами відеонагляду.

Поява нових інформаційних технологій і розвиток потужних комп'ютерних систем зберігання і обробки інформації підвищили рівні захисту інформації та викликали необхідність в тому, щоб ефективність захисту інформації росла разом зі складністю архітектури зберігання даних. Так поступово захист економічної інформації стає обов'язковою: розробляються всілякі документи щодо захисту інформації; формуються рекомендації щодо захисту інформації; діє Федеральний Закон про захист інформації, який розглядає проблеми захисту інформації та завдання захисту інформації, а також вирішує деякі унікальні питання захисту інформації.

Таким чином, загроза захисту інформації зробила засоби забезпечення інформаційної безпеки однієї з обов'язкових характеристик інформаційної системи. На сьогоднішній день існує широкий спектр пристроїв, для побудови системи відеоспостереження.

Література:

1. Aggarwal C. Neural Networks and Deep Learning / Charu C. Aggarwal. – Yorktown Heights, USA: Springer International Publishing AG, 2018. – 512 p.

2. Top 6 Deep Learning Models You Should Master for Killer AI Applications [Електронний ресурс] – Режим доступу до ресурсу: https://towardsdatascience.com/top-6-deep-learning-models-you-should-master-for-killer-ai-applications-13c7dfa68a3.

3. Computer Vision Applications: How Real-Time Image Processing is Reshaping Industries and How Your Business Can Leverage It [Електронний ресурс] – Режим доступу до ресурсу: https://perfectial.com/blog/computer-vision-applications/.

ВИКОРИСТАННЯ СИСТЕМИ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ В АНТИ-ФОРЕНЗИЦІ

Макаренко Антон Олегович
Харківський національний економічний університет ім. Семена Кузнеця
м. Харків

Форензік - прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів. [1] Форензіка розподіляється на наступні види.

Computer forensics - до неї відноситься все, що пов'язано з пошуком артефактів злому на локальній машині: аналіз RAM, HDD, реєстру, журналів ОС і так далі. [2]

Network forensics має відношення до розслідувань в області мережевого стека - наприклад, дампи і парсингу мережевого трафіку.

Forensic data analysis присвячена аналізу файлів, структур даних і бінарних послідовностей, що залишилися після атаки або використовувалися при вторгненні.

Mobile device forensics займається всім, що стосується особливостей отримання даних з мобільних пристроїв.

Hardware forensic - експертиза апаратного забезпечення і технічних пристроїв. Цей напрямок найменш популярне і найбільш складно. Сюди входить розбір даних на низькому рівні (BIOS), пошук специфічних особливостей роботи пристрою. [3]

Пропонується спосіб генерації часток секретних даних, представлених елементами секретних даних, на основі першого порога кількості часткою, які дозволяють визначати секретні дані, спосіб включає: визначення часток секретних даних на основі секрету. елементи даних, один або кілька елементів випадкових даних, доданих до елементів секретних даних, і коефіцієнти систематичного коду з поділом на максимальну відстань (MDS). [4]

Перший елемент може бути заснований на сумі двох перших часткою, а другий елемент може бути заснований на сумі двох друге часткою.

$$\begin{vmatrix} E_1^1 & E_1^2 & 0 & \cdots & 0 \\ E_1^1 + E_2^1 & E_1^2 + E_2^2 & & \ddots & \vdots \\ \vdots & & & & 0 \\ E_1^1 + E_n^1 & E_1^2 + E_n^2 & \cdots & E_n^1 & E_n^2 \end{vmatrix}$$

де - і-я перша акція, а - j-я друга акція.

Спосіб може додатково включати: об'єднання першого елемента з другим елементом кожної пари для отримання результату об'єднання для кожної пари; визначення кількох значень комбінації для кожної пари на основі результату комбінації і вектора значень розподілу; визначення часток значень множинних комбінацій шляхом виконання вищезгаданого способу генерації часток секретних даних на основі множинних значень комбінацій для кожної пари.

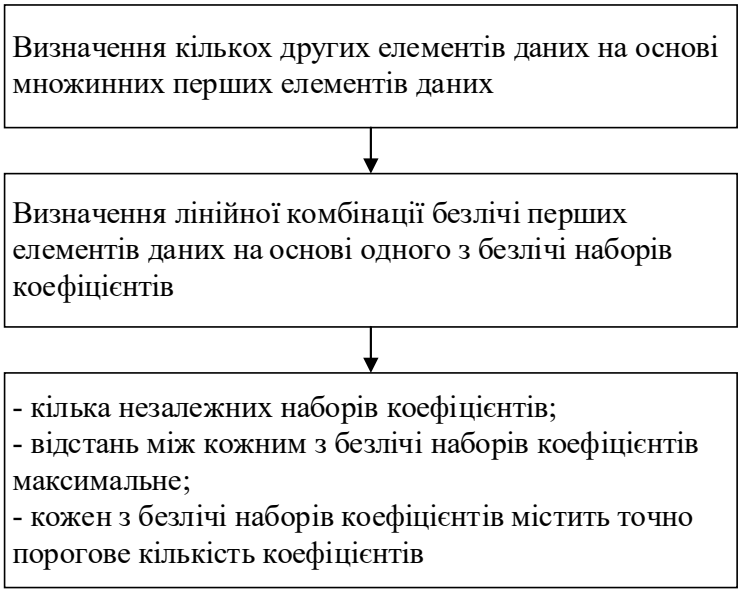


Рис 1. Спосіб спільного використання для обміну декількох елементів секретних даних.

Схема спільного використання секрету оцінюється по її безпеки - що жоден загальний ресурс не може розкрити інформацію, точність відновлення, чи буде секрет точно відновлений без будь-яких змін в порівнянні з оригіналом.

Запропоновано метод підвищення безпеки критично важливих даних, який може допомогти безпечно передавати дані, тим самим ставши важливим інструментом анти-форензіки.

Література:

1. Hor Cheong Wai. RESEARCH IN COMPUTER FORENSICS / Hor Cheong Wai. // NAVAL POSTGRADUATE SCHOOL. – 2002. – С. 205.

2. M P. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance / Рабин М, 1989. – С. 335–348.

3. Федотов М. М. Форензіка - комп'ютерна криміналістика / Микола Миколайович Федотов. – Москва: Юридический Мир, 2007. – 340 с.

4. Шелупанов А. А. Форензік. Теорія і практика розслідування кіберзлочинів / А. А. Шелупанов, А. Р. Смоліна., 2018. – 104 с

ХМАРНИЙ ГЕЙМІНГ

Миколаєнко Дмитро Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

***Хмарний геймінг**, іноді називають геймінг по вимозі, є одним з видів онлайн геймінгу. В даний час існує два основних типи хмарного геймінгу: хмарний геймінг, що базується на стримінгу потокового відео і хмарного геймінгу на основі стримінгу потокового файлу. Хмарний геймінг покликаний забезпечити кінцевим користувачам пряму здатність грати ігри на різних пристроях без затримок залежних від начинки пристрою.*

Хмарний геймінг це загальний термін, використовуваний для опису форми розповсюдження онлайн гри. Найбільш поширені методи хмарного геймінгу в даний час це — стримінг відео і стримінг файлів.

«Хмарний геймінг», а також в деяких випадках званих «геймінг по вимозі», є одним з видів онлайн геймінгу, що дозволяє прямий стримінг і стрімінг по вимозі потокового відео ігор на комп'ютерах, консолях і мобільних пристроях, подібний до відео за запитом, за рахунок використання тонкого клієнта. Сама гра зберігається, виконується, і відмальовується на віддаленому сервері оператора або ігрової компанії і відео результат стріміться безпосередньо в комп'ютер споживача через Інтернет. Це дозволяє отримати доступ до ігор без необхідності косолі і в значній мірі робить можливості комп'ютера користувача неважливими, оскільки сервер це система, яка виконує всі операціїю Управління і натискання кнопок від користувача передаються безпосередньо на сервер, де вони записані, а потім сервер посилає назад відповідь гри на управління. Компанії, які використовують цей тип хмарного геймінгу включають Playkey, PlayGiga, CiiNOW, Ubitus, Playcast Media Systems, Gaikai і OnLive.

Геймінг по вимозі це ігровий сервіс, який використовує переваги широкосмугового зв'язку, великих серверних кластерів, шифрування і стиснення потокової передачі вмісту гри у пристрій абонента. Користувачі можуть грати в ігри без завантаження або установки самої гри. Ігровий контент не зберігається на диск користувача і виконання ігрового коду в основному відбувається на серверному кластері, так що абонент може використовувати менш потужний комп'ютер, щоб грати в гру яка має більші вимоги, оскільки сервер робить всі важкі операції які зазвичай виконуються за допомогою комп'ютера кінцевого користувача. Більшість хмарних ігрових платформ закриті і запатентовані; перша хмарна ігрова платформа

з выдкритим вихыдним кодом не була випущена аж до квітня 2013 року.

Пропускна здатність бездротових мереж, затримки - основні фактори, які впливають на якість гри, оскільки дані обробляються в дата-центрі сервісу, після чого готовий відеопотік передається на пристрій користувача.

Чим якісніше зв'язок, тим плавніше картинка і вище дозвіл зображення. Якщо раніше домогтися гарної якості можна було тільки при Ethernet-підключення, то зараз мобільний широкосмуговий інтернет поступово звільняє гравців від проводів. Завдяки проникненню 5G хмарні гри стають доступнішими. Мережі п'ятого покоління дозволяють запускати сервіси типу Google Stadia і Playkey не тільки на ПК і ноутбуках, а й на мобільних пристроях в будь-якому регіоні, де є 5G покриття. У геймерів з'являється можливість грати в тайтли класу ААА по дорозі в аеропорт, в кафе, та й просто на лавочці в парку, якщо виникне таке бажання. Фактично, на руках у користувачів мобільних девайсів - мільйони ігрових гаджетів.

Незважаючи на те, що для позначення хмарного гейминга іноді використовуються терміни «стрімінг ігор» або «гри за запитом», порівняння цієї послуги з відеосервісу типу Netflix некоректно. Загальна в них тільки те, що користувач в обох випадках отримує на екран свого пристрою відеопотік з віддаленого сервера. Цінність у цих послуг різна: Netflix здає в оренду контент, а хмарний геймінг - потужне «залізо». Ігри треба запускати з аккаунта Steam, Origin або грати в безкоштовні типу Fornite, War Thunder. При цьому на ринку є підписки на каталоги ігор, наприклад Apple Arcade і Origin Play. Їх, мабуть, можна порівнювати з класичними платформами відео за запитом, але до хмарного геймінгу вони відношення не мають. Учасники ринку і власники хмарних ігрових сервісів виділяють кілька переваг послуги.

1. Хороший ігровий комп'ютер коштує від 20-30 тис. гривень і багатьом українцям не по кишені. Але будь-хто може дозволити собі грати в сучасні ігри завдяки хмарному геймінгу.

2. шерінгову економіка стає все популярнішим: навіть росіяни, готові купити гарне «залізо», скоріше, зволіють взяти його в оренду під певні завдання.

3. За рахунок своєї простоти клаудгеймінг допомагає залучити до ігор нову аудиторію, наприклад жінок.

4. Дозволяє боротися з піратством: клаудгеймінговие сервіси пропонують доступ до ліцензованих копій ігор.

5. «Великі» гри практично не випускають для macOS, але завдяки хмарному геймінгу в них зможуть грати і користувачі «яблучної» техніки.

6. Коли з'являться мережі 5G, грати в вимогливі ігри можна буде де завгодно, хоч у дорозі на роботу або навчання.

Хмарними іграми зацікавилися найбільші компанії світу, включаючи Microsoft, Google, Amazon, Nvidia, Sony, Tencent, NetEase. Учасників ринку стає все більше. Наприклад, компанія Amazon пообіцяла в цьому році запустити власну ігрову платформу "Project Tempo". Активно розширюється ніша хмарних ігор в Азії. Так, в березні 2020 року компанії Sanqi Interactive Entertainment і Huawei Cloud домовилися спільно розвивати платформу хмарного гейминга. Не відстає і Росія. Зараз в країні доступні: GeForceNow. Playkey. Loudplay. Megadrom. Power Cloud Game. Drova.

В цілому оператори і експерти позитивно налаштовані по відношенню до хмарного геймінгу, але скоріше схильні бачити в ньому перспективу, яка дозволить заробляти в майбутньому

«Хмарний геймінг - це все ж план на майбутнє. Такі сервіси, як xCloud або GeForce Now є комплементарними до традиційного геймінгу і поки не прагнуть його замінити. З вдосконаленням самої технології хмарного гейминга і інфраструктурних технологій, наприклад гигабитного інтернету, 5G, в якийсь момент можна припустити, що цей спосіб стане основним.

Література:

1. *https://uk.wikipedia.org/wiki/Хмарний_геймінг*
2. *https://habr.com/ru/post/520364/*
3. *https://telesputnik.ru/materials/tech/article/est-li-perspektivy-oblachnogo-geyminga-dlya-operatorov-svyazi/*

ВІРТУАЛЬНІ АСИСТЕНТИ

Минько Євгеній Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Віртуальні асистенти в майбутньому будуть невід'ємною частиною сучасного життя.

Сучасні інформаційні технології стрімко розвиваються. Одним із головних напрямків є штучний інтелект, останнім часом дуже багато розвинених країн інвестують у його розвиток. Станом на сьогодні лідером у розвитку штучного інтелекту є США . Щороку захищається близько 2000 докторських

дисертацій і засновується близько 1500 стартапів у галузі штучного інтелекту. Незважаючи на лідерство США також в цій індустрії за перевагу бореться і Китай.

Штучний інтелект і Україна. Згідно з даними дослідження, проведеного компанією Deep Knowledge Analytics в 2019 році, Україна була одним із лідерів в Східній Європі в області розвитку штучного інтелекту. Тоді наголошувалося, що кращими школами ШІ за межами Кремнієвої долини вважаються російські, українські та білоруські. Ці країни є глобальним джерелом інновацій в області штучного інтелекту і пов'язаними з ним технологіями. У дослідженні повідомлялося, Росія, Білорусь і Україна – це країни, які отримують найбільшу кількість грантів на розробку ШІ, перемагають у конкурсах і отримують інвестиції.

Історія розвитку голосових асистентів

Історія голосових асистентів розпочалася в 1930-х роках, коли вперше вчені намагалися розпізнати голос людини використовуючи комп'ютерні технології. Тоді створенню якісного асистента заважали два чинники: існування омонімів та постійний шумовий фон, із якого система повинна обирати голос користувача. Зараз для вирішення цих проблем розробники використовують машинне навчання. Воно навчає нейронні мережі самостійно аналізувати контекст та ефективно вираховувати джерело виникання звуку. Однак прийшли розробники до цього не одразу – потрібно було витратити близько 80 років на підготовчі роботи.

1939 рік. Радянський фізик Лев Мясников створив апарат, спроможній розпізнати людську мову – декілька голосних та приголосних звуків.

1952 рік. Співробітники лабораторії Bell розробили механізм, котрий розпізнавав продиктовані по телефону числа від одного до дев'яти.

1962 рік. Компанія IBM представила особисту технологію розпізнання голосу – Shoebox. Машина розпізнавала 16 англійських слів, 10 цифр та 6 арифметичних команд.

1980 рік. Інженери навчилися застосовувати методи «скритої технології Маркова». З часом це дало можливість голосовим системам краще розпізнавати людську мову. Вони опрацьовували слово, враховуючи декілька попередніх і враховує можливі варіанти продовження речення. Скрита модель Макарова описує генерацію випадкових подій в залежності від теперішнього стану об'єкту. Наприклад: якщо людина лежить, но вона не може моментально перейти кудись – потрібно встати і тільки потім йти.

1987 рік. В США компанія Worlds of Wonder почала продавати ляльку, що розмовляє під час гри вона вчилася розпізнавати голос дитини. В ляльку був влаштований процесор, котрий давав їй можливість реагувати і створювати репліки. Вона сприймала вісім висловлювань: «Джулі», «так», «ні», «добре», «вдавати», «голодна», «співай» та «мовчи».

1990 рік. З'явилася комерційна програма Dragon Dictate, орієнтована на масовий ринок. Вона розпізнавала мову та записувала надиктований текст в файл.

1996 рік. З'явилося повноцінне голосове меню VAL від BellSouth. Система опрацьовувала телефонні довідники і допомагала покупцям в пошуку потрібної інформації про товари. Пізніше компанія запустила Info by Voice – інтерактивні голосові помічники з інформацією про найближчі ресторани, таксі і деякі магазини. Система також могла розповісти про новини і акції, погоду та телепрограму, спортивні новини та гороскоп.

2001. Компанія Microsoft додала голосовий ввід тесту в офісний пакет Office XP.

2002 рік. Google запустили Voice Search – сервіс для голосового пошуку в інтернеті. Проект призупинили через незручність користування. На базі Voice Search заснований сучасний інтерактивний помічник - Google Assistant.

2007 рік. Цент вивчення штучного інтелекту SRI International почав розробку Siri. Siri стала першою голосовою асистенткою – система вміла не тільки шукати інформацію в інтернеті чи працювати як голосове меню, але й вести з користувачем діалог.

2011 – 2014 роки. Google інтегрував функцію голосового пошуку в браузері Chrome. Компанія також запустила персоналізованого асистента Google Now з розширеними можливостями голосового пошуку – сервіс підбирав актуальну інформацію враховуючи місцезнаходження користувача, історії браузеру та інших пошукових запитів.
У Microsoft також з'явилася особиста віртуальна голосова помічниця Cortana.

2014 рік. Amazon представив першу у світі розумну портативну колонку Amazon Echo з голосовою помічницею Alexa.

2017 рік. Alibaba представили розумну колонку Tmall Genie з голосовим асистентом AliGenie.

2018 рік. Яндекс випустили розумну колонку Яндекс.Станція з голосовою помічницею Алісою.

Як влаштовані сучасні голосові помічники

Голосові помічники пасивно зчитують всі звукові сигнали, та для активної роботи їм необхідна активація за допомогою кодової фрази. Наприклад, скажіть : «Окей, Google», потім можете задати своє питання чи дати команду без пауз. В момент голосового запиту автоматично система розпізнавання голосу перетворить звуковий сигнал в тест. Це відбувається в чотири етапи:

1) Фільтрація. Система прибирає із звукового сигналу шумовий фон та всі перешкоди, утворені в момент запису.

2) Оцифровування. Звукові хвилі перетворюються в зрозумілий для комп'ютера цифровий формат. Параметри отриманого коду в тому рахунку визначають якість запису.

3) Аналіз. В сигналі виділяються проміжки, що містять людську мову. Система оцінює її параметри - до якої частини мови відноситься слово, в якій воно формі, наскільки можливий зв'язок між двома словами.

4) Виявлення шаблонів даних. Отриману інформацію система додає в словник – збирає різні варіанти вимови одного і того ж слова. Для того, щоб точніше розпізнавати нові запити, асистенти порівнюють слова в них з шаблонами.

Якщо після опрацювання запиту віртуальний помічник не розуміє команду чи не може знайти відповідь, він просить перефразувати питання. В деяких випадках можуть знадобитися додаткові данні – наприклад, при замовленні таксі асистент може уточнити місцезнаходження користувача і пункт призначення.

Майбутнє голосових помічників

Найближчим часом віртуальні асистенти позбудуться обмеження рамками смартфонів чи колонок. Крупніші виробники поступово переводять своїх асистентів на приладну дошку автомобілів. Спеціально виготовлені під бізнес-задачі і продуктивність співробітників помічники мають з'явитися в офісах. Вони спростять проведення аудіо та відео конференцій, планування і виконання різних дій. Один із останніх трендів – інтеграція помічників у «розумний» дім: свої асистенти з'являються у відеокамер спостереження, термостатів і навіть побутової техніки.

Література:

1. https://blog.dti.team/voice-assistants-1/

2. https://aiconference.com.ua/uk/news/golosovie-assistenti-chto-oni-umeyut-i-chem-otlichayutsya-drug-ot-druga-97306

АКТУАЛЬНІ ПРОБЛЕМИ ІНФОРМАЦІЙНИХ

ТЕХНОЛОГІЙ В УМОВАХ ПАНДЕМІЇ COVID-19

Міхеєв Сергій Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Пандемія нової коронавірусної інфекції COVID-19 вже зробила безпрецедентний вплив на різні сфери людської життєдіяльності, в тому числі на її сучасний технологічний уклад. У цій статті будуть розглянуті актуальні проблеми в сфері інформаційних технологій в умовах пандемії вірусу COVID-19.

Спалах коронавіруса змусив багатьох людей по всьому світу працювати і вчитися вдома, а підприємства і установи - переводити свою діяльність в онлайн-середовище. Кіберзлочинці активно використовують ці непрості обставини щоб знайти нові незаконні способи заробітку. Вони розширюють і диверсифікують свою діяльність, користуючись атмосферою страху і невизначеності.

1. Фактори, що впливають на кібербезпеку

Європол (Агентство по співпраці правоохоронних органів Європейського союзу) виділяє основні чинники, які впливають на рівень кіберзлочинності:

- високий попит на певні товари, захисні засоби та фармацевтичну продукцію;
- зниження мобільності громадян;
- громадяни залишаються вдома і все частіше працюють на дому, використовуючи цифрові рішення;
- обмеження в суспільному житті роблять деякі злочинні дії менш помітними і переносять їх в онлайн-простір;
- збільшення рівня тривожності в суспільстві;
- скорочення поставок певних товарів.

2. Кібератаки: шкідливі домени, зловмисні програми та вимагання в мережі

Шкідливі домени. Кіберзлочинці кожен день створюють тисячі сайтів, які містять слова «коронавірус», «COVID-19», різні варіації написання цих термінів і використовують їх для проведення спам-кампаній, фішингу, поширення зловмисних програм або злому серверів управління і контролю.

Зловмисне програмне забезпечення. Кіберзлочинці користуються популярністю повідомлень про коронавіруси для маскування своєї діяльності. Шкідливі, шпигунські та троянські вірусні программи зазвичай представлені під виглядом інтерактивних карт і веб-сайтів про коронавірус. Спам-повідомлення також змушують користувачів переходити за посиланнями, які завантажують шкідливе ПО на комп'ютери або мобільні пристрої.

Вимагання. Кіберзлочинці піддають сервери лікарень, медичних центрів і державних установ атакам і вимаганню. Установи, що знаходяться на передньому краї боротьби з коронавірусом, що зіштовхуються з безпрецедентною загрозою для здоров'я, тепер також протистоять ще одній загрозі - з боку кіберзлочинців. Їх доступ до життєво важливих файлів і систем виявляється заблокованим до тих пір, поки не буде виплачений викуп. Оскільки в умовах кризи в галузі охорони здоров'я лікарні не можуть дозволити, щоб їх системи були заблоковані, вони змушені платити злочинцям. Блокування роботи лікарень і їх критичних систем не тільки затримує оперативну медичну діяльність, таку необхідну в період пандемії, але і може безпосередньо привести до смертельних випадків. Програма-вимагач може проникнути в системи через електронні листи, скомпрометовані облікові дані співробітників або за допомогою вразливості в системі.

Кіберзлочинці, ймовірно, будуть прагнути використовувати все більше число нових способів атак, оскільки все більше роботодавців вводять дистанційний режим роботи і встановлюють віддалене підключення до своїх систем для співробітників.

3. Шахрайство і контрафактна торгівля засобами індивідуального захисту та противірусними лікарськими засобами.

Крім виключно «цифрових» злочинів на тлі пандемії загострюються і раніше існували проблеми, які перейшли в електронний формат. Зловмисники дуже швидко адаптували відомі схеми шахрайства до нових умов, щоб отримати вигоду з кризи, пов'язаної з пандемією COVID-19.

Продаж через Інтернет контрафактної медичної продукції. Оскільки попит на засоби індивідуального захисту і гігієни зростає в геометричній прогресії, злочинці прагнуть отримати прибуток, продаючи неякісні або контрафактні товари, такі як хірургічні маски, дезінфікуючі засоби, противірусні та протималярійні препарати (включаючи неіснуючі ліки від COVID-19), вакцини, тест-набори для аналізу на коронавірус.

Фінансове шахрайство. Оскільки хірургічні маски та інше медичне приладдя користуються великим попитом, але їх важко знайти в роздрібних магазинах, в Інтернеті з'явилися підроблені магазини, веб-сайти, облікові записи в соціальних мережах, що нібито торгують цими товарами. Але після перерахування оплати товари покупцеві не відправляються.

4. Інформаційні загрози в епоху COVID-19.

У той час як соціальні мережі корисні для обміну інформацією, вони також стають джерелом «фейковий новин». Компанії намагаються докладати зусиль для боротьби з негативним феноменом.

Окремий вид загроз пов'язаний зі зростаючою навантаженням на цифрові сервіси та технології. Так, разом зі стрімким зростанням аудиторії деякі сервіси зіткнулися зі складнощами, спричиненими різким збільшенням навантаження на їх технологічні можливості.

Глобальний Інтернет зіткнувся з безпрецедентним зростанням трафіку в умовах масштабного переходу населення до віддаленої роботи та навчання, однак його пропускна здатність поки змогла задовольнити всі зростаючі потреби. Почасти це пояснюється тим, що максимальна продуктивність каналів зв'язку була розрахована і підготовлена таким чином, щоб задовольняти масове використання сервісів потокового відео типу Netflix в пікові вечірні години. Однак в технологічному плані пропускна здатність Інтернету не безмежна, що може становити загрозу в разі несприятливого подальшого розвитку ситуації.

5. **Заходи, що вживаються для пом'якшення наслідків і захисту критично важливої медичної інфраструктури**.

Інтерпол допомагає країнам-членам розслідувати кібернапади на лікарні і пом'якшувати їх наслідки. Щоб підтримати глобальні зусилля по боротьбі з цією критичною небезпекою, організація випустила повідомлення, яке попереджає поліцію всіх 194 країн-членів про посилення загрози кібервимогання. Крім того, Інтерпол формує список підозрілих інтернет-доменів, пов'язаних з COVID 19, проводить їх подальший аналіз і оцінку, взаємодіє з відповідними країнами для вжиття заходів. Група реагування на загрози кіберзлочинності Інтерполу стежить за всіма кіберзагрозами, пов'язаними з COVID-19, тісно співпрацюючи з приватними партнерами в галузі кібербезпеки, щоб збирати інформацію і надавати підтримку організаціям.

6. Заходи профілактики.

Група реагування на комп'ютерні інциденти в рамках інститутів, установ і органів Європейського союзу (CERT-EU) вживає заходи для оцінки цифрових аспектів короновірусної пандемії. Група включає експертів з інформаційної безпеки з основних інститутів ЄС. Вона розробила план усунення будь-якої потенційної загрози, яка може вплинути на кібербезпеку і інтереси інститутів, установ і органів ЄС: «Гід по кібербезпеці: як пережити пандемію COVID-19». Гід описує картину

кіберзагроз та дає перелік конкретних заходів, які можуть допомогти підприємствам і установам подолати кризу і запобігти наслідкам кібератак:

1. *Встановити зв'язок*

1.1. Встановити чіткі внутрішні канали зв'язку між інфраструктурою, групою безпеки і керівництвом і регулярно контролювати їх. Визначити безпечні резервні канали зв'язку, якщо існуючі IT-системи, які використовуються для цієї мети, недоступні.

1.2. Дізнатися про способи зв'язку з державною групою реагування на інциденти в області комп'ютерної безпеки.

1.3. Переконатися, що є доступ до всіх засобів зв'язку з державною групою реагування на інциденти в області комп'ютерної безпеки, щоб скоротити час відгуку і підвищити ефективність.

2. *Визначити відповідних стейкхолдерів*

2.1. У своїй організації.

2.2. У своєму секторі підприємництва.

2.3. Включити державну групу реагування в свій план реагування на кризу.

3. *Встановити процес реагування на інциденти*

3.1. Встановити внутрішній процес реагування на інциденти, включаючи процедури, ключових співробітників та інструменти, які дозволили б здійснювати цей процес.

3.2. Знати про будь-які можливі каскадні наслідки порушення кібербезпеки.

3.3. Ознайомитися з механізмами повідомлення про інциденти державної групи реагування.

7. Висновки.

Пандемія коронавірусу дала потужний імпульс масовому впровадженню цифрових технологій в повсякденне життя. Вже зараз очевидно, що зміни, які ця тенденція внесе в суспільно-економічний уклад, будуть носити безпрецедентний характер. Тривалі в більшості країн світу заходи щодо соціальної ізоляції змусили перейти в онлайн істотну частину світової торгівлі товарами і послугами. Ймовірно, незабаром світ буде спостерігати подальше вибухове зростання капіталізації постачальників онлайн-послуг на тлі падіння позицій компаній сировинних галузей. Кардинально зміняться моделі споживання. Помітна частка роботи і освіти також піде в дистанційний формат.

З одного боку, ці зміни зроблять життя людини ще більш зручним. Широкі горизонти для розвитку людства відкриває можливість не виходячи з дому забезпечувати себе необхідними

потребами, задіяти для виконання ряду «непрестижних» або небезпечних завдань робототехніку, отримувати необхідну інформацію про основні соціально-економічні тенденції в форматі відкритих даних, лікувати захворювання і протидіяти їх поширенню за допомогою технологій дистанційної взаємодії, використання штучного інтелекту і аналізу великих даних.

Проте існує величезний набір ризиків і питань, на які поки немає однозначної відповіді. Як забезпечити приватність і захист персональних даних в умовах активної цифровізації життя? Як забезпечити права і свободи, підтримка яких стала чи не центральною ідеологією для всього світу протягом другої половини XX століття, коли пересування громадян жорстко фіксуються і регулюються в рамках заходів по ізоляції? Як вирішити комплекс проблем, пов'язаних з кібербезпекою при тому, що дедалі більша частина нашого повсякденного життя буде переведена в онлайн-режим?

Відповідь на ці питання дасть лише подальший розвиток подій. Але вже зараз є підстави вважати, що поточна криза в зв'язку з COVID-19 стане передвісником одного з найбільших переформатувань політичного і соціально-економічного укладу в сучасній історії. Провідну роль в ньому гратимуть саме цифрові технології, а в стороні від нього, ймовірно, не залишиться практично жодна держава світу.

Література:

1. The COVID-19 Crisis: Accentuating the Need to Bridge Digital Divides [Електронний ресурс] URL: https://unctad.org/system/files/official-document/dtlinf2020d1_en.pdf (Дата звернення: 11.02.2021)

2. Цифрові технології та кібербезпека в контексті поширення COVID-19 [Електронний ресурс] URL: https://ach.gov.ru/upload/pdf/Covid-19-digital.pdf (Дата звернення: 11.02.2021)

3. How criminals profit from the COVID-19 pandemic [Електронний ресурс] URL: https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic (Дата звернення: 11.02.2021)

ОСОБЛИВОСТІ ПАРАДИГМИ ПЕРИФЕРІЙНИХ ОБЧИСЛЕНЬ (EDGE COMPUTING)

Мутьянов Володимир Михайлович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

1. **Постановка задачі** - ознайомити слухачів із парадигмою периферійних розподілених обчислень, її специфікою, перевагами та недоліками.

2. **Мета дослідження** - донести інформацію по темі, розділивши її на 4 пункти:

1) Що таке периферійні обчислення?
2) Особливості архітектури периферійних обчислень.
3) Приклади використання технології периферійних обчислень.
4) Проблеми та переваги впровадження технологій.

3. Результати дослідження.

Периферійні (граничні) обчислення – це парадигма розподілених обчислень, здійснюваних в межах досяжності кінцевих пристроїв. Даний підхід використовується для скорочення часу відклику мережі та більш ефективного використання пропускної здатності мережі.

Наразі існує декілька підходів до описання концепції граничних обчислень. Наприклад, одним із визначень граничних обчислень вважають будь-яку комп'ютерну програму будь-якого типу, що забезпечує більш низьку мережеву затримку у рамках використання кінцевих приладів

У своїх виступах доктор Карим Арабі означив периферійні обчислення як усі обчислення, що відбуваються за межами хмари, але в межах мережі, кажучи більш точно – у додатках, де необхідна обробка даних в реальному часі. Згідно з даним визначенням, хмарні обчислення працюють із великими даними (Big Data), в той час як граничні обчислення оперують так званими «миттєвими даними», тобто даними в реальному часі, що генеруються датчиками пристроїв або користувачами.

Згідно з даним означенням, можна зробити висновок, що головна відмінність граничних обчислень від хмарних обчислень полягає в тому, що у першому випадку збір та аналіз даних здійснюється на місці генерації потоку даних, в той час як використання централізованих систем передбачає подальшу передачу інформації в центр обробки даних, таким чином збільшуючи час обміну та обробки даних.

Зростання кількості пристроїв інтернету речей (IoT) призводить до створення масивних обсягів інформації, яку необхідно передати на аналіз в дата-центри, таким чином підштовхуючи можливості пропускної здатності мереж до їх меж. Незважаючи на покращення мережевих технологій, централізована обробка інформації не здатна забезпечити прийнятну швидкість передачі та обробки даних для багатьох сервісів. Крім того, пристрої на межі мережі постійно споживають дані, таким чином змушуючи компанії до побудови мереж доставки інформації для децентралізації даних та забезпечення надання послуг, коректуючи фактор відстані до кінцевого користувача.

Схожим чином метою граничних обчислень є перенесення обчислювальних навантажень із дата-центрів на межу мережі за рахунок використання обчислювальних потужностей розумних пристроїв, мобільних телефонів або мережевих шлюзів для виконання операцій від імені хмари.

Децентралізуючи обчислення, перенісши їх на периферійні пристрої стає простішим завдання обчислення даних додатків, для яких критичним параметром є затримка отримання даних, таких як автоматизований транспорт. Знижуючи мережні затримки знижується шанс несвоєчасного здійснення маневру транспортом, що потенційно підвищує безпечність автономного транспорту.

Децентралізований підхід граничних обчислень дозволяє знизити обсяг даних, що передається мережею. Опрацювання даних починається поруч із місцем їх збору, і тільки дані, які необхідно зберегти відправляються до хмарного сховища. Це збільшує можливості масштабування і ефективність граничних обчислень та знизити навантаження на мережу. Прикладом можна взяти передачу відео-матеріалів із багатьох камер спостереження, що призводить до зниження пропускної здатності мережі. Більш явною ця проблема стає в сценарії використання широких мереж інтернету речей, де дані генеруються тисячами сенсорів із різних пристроїв.

Підвищення відмовостійкості та зниження переривів з’єднання також є результатом периферійних обчислень, оскільки цей підхід не залежить виключно від хмарних обчислень. Це може допомогти в уникненні простою сервера в разі несправності, забезпечивши надійну роботу сервісу у віддалених місцевостях та запобігти незапланованому простою через несправність.

Теоретично, децентралізація обчислень додає додатковий рівень безпеки до мережі, оскільки велика кількість даних від приладів інтернету речей не передається глобальною мережею. Менше даних у хмарному сховищі – менше даних, що можуть бути розкриті в разі витоку.

Проте, незважаючи на це, є побоювання щодо вразливості периферійних мережевих пристроїв, оскільки відомі випадки використання вразливостей в пристроях IoT, що потенційно створює сотні несанкціонованих точок доступу до мережі. Ця вразливість буде підштовхувати використання шифрування інформації, методів контролю доступу таVPN-тунелювання.

Процес переходу від хмарних обчислень до периферійних обчислень або гібридного підходу (використання периферійних та хмарних обчислень для завдань із різними потребами) може

значно пришвидшитись із поширенням бездротових технологій 5G, що забезпечить значний приріст пропускної здатності мобільних мереж.

Необхідність проведення обчислень на вимогу та взаємодії з додатками в режимі реального часу разом із покращенням технологій бездротової передачі даних грають значну роль у поширенні розподілених обчислень.

Незважаючи на те, що головною метою периферійної обробки даних було зниження навантаження на пропускну здатність для пристроїв IoT на великих відстанях, ріст в кількості операцій в реальному часі що потребують локальних обчислень та місця для зберігання будуть підштовхувати цю технологію в найближчі роки.

Література:

1. https://en.wikipedia.org/wiki/Edge_computing

2. https://www.cloudwards.net/what-is-edge-computing/

3. https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html

PYTHON ЯК ІНСТРУМЕНТ ПОЛЕГШЕННЯ ЖИТТЯ ДЛЯ СИСТЕМНОГО АДМІНІСТРАТОРА

Назаренко Дмитро Олександрович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Кожний системний адміністратор в своїй роботі стикався з проблемою купи однакових дій для рішення тривіальної задачі. Будь то адміністратор мережі провайдера, який провіряє надходження пакетів від користувача мережі, чи адміністратор дата центру, який слідкує за показниками температур, роботи жорстких дисків і так далі. Повторення однакових рухів допомагає на початку роботи для її засвоєння, але не після року праці. Це лише додає нудьги та лишніх клопотів. Тому було багато створено скриптів, програм та утиліт для полегшення роботи, такі як звичайний ping чи traceroute.

Але все ж остаються процеси які можуть бути автоматизованими, але вони є локальними для компаній чи підприємств в яких і працюють адміністратори. Компанії можуть найняти команди розробників для створення інструментів для пришвидшення роботи чи введення нового методу роботи. Провайдери зазвичай роблять базу даних клієнтів і зв’язують її з сервером DHCP і таке інше. Але попри велику кількість автоматизованих процесів, ще лишаються такі тривіальні речі як перевід MAC адрес в різні формати для різних комутаторів та маршрутизаторів чи перевірка лог-файлів серверу на помилки. Тому, на мою думку, кожний адміністратор

повинен знати хоча б один скриптовий язик програмування такий як Python, Bash чи Perl.

По-перше, я взяв до уваги Python, бо він буде універсальним для багатьох систем, таких як сервери Linux чи Windows. Також він простий у вивченні, його відносно легко читати та має величезну базу сторонніх та внутрішніх інструментів.

По-друге, великі виробники мережевого обладнання, такі як Cisco, Juniper, Huawei, впроваджують підтримку Python на своєму обладнанні. У мови є майбутнє в мережевий сфері, і його вивчення не буде марною тратою часу.

Для того, щоб почати вивчати Python знань про програмування не треба. На офіційному сайті є всі потрібні речі. Мінімум інструментів – це інтерпретатор з офіційного сайту та текстовий редактор. Так як, більшість адміністраторів добре знайома з CLI, для запуску скриптів проблем не зіставить введення команди python3 [назва програми].py . На сайті www.python.org також є навчальний курс по основам мови та стандартній бібліотеці. Не буде лишнім додати, що є дуже корисні python проекти такі як pylint, venv, pip та pdb.

Pylint – програма для перевірки стилю написання коду та його оцінки. В PEP 8 описані правила по оформленню стилю коду від самого автора мови. Програма буде оцінювати наскільки схожий код на описаний в документі від 0 до 10 з помітками, де краще виправитися.

PDB – аналізатор коду на предмет фізичних та логічних помилок, перевірку використання пам’яті і таке інше.

VENV – програма по створення віртуального простору, для створення проектів та їх використання, щоб не завадити всій системі при помилках чи не коректній роботі.

Ну і **pip** – де факто програма для всіх систем на python для завантаження сторонніх модулів.

Висновок:

У висновку я хотів би сказати, що такі мови як Python можуть повністю забрати на себе практично всю роботу при грамотному використанні.

Література:
1. *www.python.org*
2. *docs.python.org/3*

СТЕК УТИЛІТ МЕРЕЖЕВОГО АДМІНІСТРАТОРА

Назаренко Дмитро Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Для якісної і безперебійної роботи мережі - як локальної, так і зовнішньої - потрібно своєчасно проводити її моніторинг і діагностику. Трапитися може що завгодно, починаючи з крадіжки трафіку і закінчуючи потраплянням в її середовище вірусних програм. Щоб цього не сталося, адміністратор повинен здійснювати регулярний збір мережевих даних, вивчати поточні показники і вживати відповідних заходів у разі виявлення несправностей. Для цього в його не легкій справі використовуються мережеві утиліти. В цій роботі я буду використовувати лише утиліти сімейства операційних систем Windows, хоча для більшості систем різниця лише в назвах утиліт.

Утиліта ping. Ping в своїй роботі використовує протокол ICMP і призначена для перевірки з'єднання з віддаленим хостом. Перевірка з'єднання здійснюється шляхом посилки на адресу хоста спеціальних ICMP-пакетів, які відповідно до протоколу повинні бути повернуті відправнику (ехо-пакети та ехо-відповіді). В самому простому випадку так буде виглядати команда:

ping hostname, де hostname - NetBIOS або DNS - ім'я хоста або його IP-адресу.

Утиліта tracert. Як і утиліта ping, tracert використовує ICMP протокол для визначення маршруту до пункту призначення. В результаті роботи утиліти на консоль виводяться всі проміжні вузли маршруту від вихідного хоста до пункту призначення і час їх проходження. Команда виглядає так:

tracert hostname, де hostname - NetBIOS або DNS- ім'я хоста або його IP-адресу.

Утиліта ipconfig. Ipconfig є найбільш поширеною мережевий утилітою. З її допомогою можна визначити конфігурацію IP-інтерфейсу і значення всіх мережевих параметрів. Особливо ця утиліта корисна на комп'ютерах, що працюють з протоколом DHCP: команда дозволяє перевірити параметри IP-інтерфейсів встановлені в автоматичному режимі. Вигляд команди: **ipconfig**

Утиліта nslookup. Nslookup призначена для перевірки правильності роботи DNS-серверів. За допомогою утиліти, користувач може виконувати запити до DNS-серверів на отримання адреси хоста по його DNS-імені, на отримання адрес і імен поштових серверів, відповідальних за доставку пошти для окремих доменів DNS, на отримання поштової адреси адміністратора DNS-сервера і т. д. Утиліта працює в двох режимах: в режимі однократного виконання (при запуску в командному рядку задається повний набір параметрів) і в інтерактивному режимі (команди і параметри задаються в режимі діалогу)._Запуск утиліти в інтерактивному режимі здійснюється запуском команди nslookup без параметрів.

Утиліта netstat. Netstat дозволяє отримати статичну інформацію по деяким з протоколів (TCP, UDP, IP, ICMP), а також інформує вас про поточні мережевих з'єднаннях. Особливо вона корисна на брандмауерах, з її допомогою можна виявити порушення безпеки периметра мережі. Вигляд команди: **netstat**

Утиліта arp. Утиліта використовується для перегляду і модифікації ARP-таблиці, використовуваної для трансляції IP-адрес в адреси протоколів канального рівня (MAC-адреси). За допомогою параметрів команди можна роздруковувати таблицю, видаляти і додавати дані ARP-таблиці. Коригування ARP-таблиці може здійснювати тільки користувач з правами адміністратора. Утиліта запускається з різними ключами, наприклад щоб побачити arp-таблицю команда виглядає так:

arp -a

Утиліта route. Route дозволяє маніпулювати таблицею мережевих маршрутів, яка є на кожному комп'ютері з TCP/IP-інтерфейсом. Утиліта забезпечує виконання чотирьох команд: print (роздруківка таблиці мережевих маршрутів), add (додати маршрут в таблицю), change (зміна існуючого маршруту), delete (видалення маршруту). Вигляд команди: **route print**

Утиліта hostname. Утиліта призначена для виведення на консоль імені хоста, на якому виконується дана команда. Команда hostname не має ніяких параметрів.

Утиліта pathping. А ця потужна утиліта являє собою сукупність Tracert і Ping. Відправляє дані по маршрутизаторів, використовуючи ефект луни (запит-відповідь). На підставі отриманих результатів проводить аналіз і видає чітку інфографіку.Вигляд команди: **pathping google.com**

Утиліта telnet. Це мережева утиліта, яка дозволяє з'єднатися з віддаленим портом будь-якого комп'ютера і встановити інтерактивний канал зв'язку, наприклад, для передачі команд або отримання інформації. Можна сказати, що це універсальний браузер в терміналі, який вміє працювати з безліччю мережевих протоколів. Вигляд команди: telnet 192.168.0.1

Висновок. Даний стек утиліт повинен знати кожен адміністратор мережі для виявлення, запобігання та вирішення помилок чи пошкодженнь у мережі.

Література:

1. *https://losst.ru/kak-polzovatsya-telnet*
2. *http://compbasic.ru/net-tools-windows/*
3. *http://stilus-doctus.narod.ru/netutil.html*

ЗАСТОСУВАННЯ ТА ПРИНЦИПИ БЕЗПЕКИ В СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Нікітін Олексій Геннадійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Актуальність поданої статті полягає в тому, що принципи фізичної безпеки, багато з яких можуть бути запозичені з набору перевірених принципів IT-безпеки, допомагають керівникам в питаннях створення безпечного оточення безпосередньо з того моменту, коли в цьому виникла необхідність.Висновком роботи можуть бути виробники, які повинні незмінно дотримуватися чітко визначених принципів безпеки. В даний час вони пропонують стандартний набір заходів безпеки, в той час як системи повинні бути спроектовані для конкретних завдань.

Безпека часто розглядається просто як «щось необхідне» для компанії. Відповідно кошти, вкладені в систему безпеки, розглядаються як витрати, а не як інвестиції, їх обсяг недооцінюється і применшується. В результаті багато компаній занадто пізно починають розглядати конкретні заходи безпеки, які повинні бути реалізовані. Те ж саме відноситься до інших об'єктів організацій, таких як IT-підрозділи. Тому в багатьох областях принципи розроблені в якості керівництва для прийняття бізнес-рішень.

Принципи, створені на основі передового досвіду, містять рекомендаціїдля керівників і установників обладнання компанії. Дані принципи зобов'язують зацікавлені сторони на початковому етапі сформулювати цілі і створити проект. В цьому відношенні принципи є основою протягом усього процесу покупки і впровадження придбань.

З урахуванням об'єднання сфер безпеки та IT, а також таких явищ як глобалізація, застосування нових методів роботи і технологічних розробок, до систем безпеки пред'являються все більш високі вимоги. В результаті принципи безпеки стають все більш важливими. Тому перевірені принципи безпеки беруть свій початок в сфері IT-безпеки.

Принципи безпеки можна визначити, як набір бажаних властивостей системи, моделей поведінки, цілей і методів впровадження, які знижують ймовірність реалізації загрози і зменшують наслідки в разі її реалізації. Принципи безпеки допомагають визначити необхідні вимоги, прийняти рішення з питань архітектури та впровадження, а також виявити можливі вразливі місця систем. Вони допомагають керівникам в питаннях створення безпечного оточення безпосередньо з того моменту, коли в цьому виникла необхідність. Вони мотивують постачальників критично ставитися до питання і постійно

перевіряти рішення, прийняті в процесі придбання та впровадження засобів безпеки.

Варто застосовувати «глибокий» захист. Це означає, що необхідні багаторівневі заходи безпеки. Ніхто не повинен покладатися тільки на один рубіж захисту. Публічний доступ до системи повинен бути ізольований від критично важливих ресурсів, фізичні і логічні заходи повинні застосовуватися в комбінації.

Необхідно використати позитивну модель системи безпеки. Щоб забезпечити надійний контроль доступу, замість чорного списку необхідно використовувати білий список в комбінації зі значеннями за замовчуванням і мінімальними можливостями для атаки. Наприклад, необхідно використовувати зумовлені варіанти, замість порожніх полів для введення інформації.

Потрібно забезпечити реалізацію відмовостійкої політики і роботу всіх компонентів з найменшим рівнем привілеїв**.** Компоненти системи не повинні мати більше функціональних можливостей, ніж це необхідно для виконання їх завдань. Наприклад, кожен компонент повинен мати доступ тільки до тих таблиць в базах даних, які необхідні для його роботи, і не мати доступ до всіх інших таблиць або баз даних, щоб запобігти несанкціонованому доступу.

Слід уникати такого підходу, при якому безпека забезпечується за рахунок невідомості. У якісно розробленій криптосистемі тільки ключ повинен зберігатися в секреті, а використовувані алгоритми не повинні містити прихованих елементів. Для цього повинні застосовуватися контрольовані і економічно здорові механізми. Зусилля та інвестиції повинні відповідати досягнутому рівню безпеки.

Варто виявляти вторгнення**.** Переконайтеся, що ви зберігаєте всю важливу інформацію, щоб реагувати на події, як тільки вони відбуваються. Також необхідно впровадити процедури для подальшого контролю і реагування на події.

Не потрібно відноситись з довірою до інфраструктури або сервісу. Якщо будь-який зовнішній ресурс або сервіс повинен відповідати політиці організації, він повинен бути перевірений. Крім того, до всіх зовнішніх систем слід ставитися з обережністю, використовуючи аналогічні стандарти.

Необхідно створити надійні стандартні параметри. Безпека ніколи не повинна бути поставлена під загрозу в зв'язку зі зручністю використання. За замовчуванням повинні застосовуватися максимально можливі заходи безпеки. Система повинна забезпечувати реалізацію цьогопринципу, в той час як

конкретні користувачі повинні мати можливість робити винятки в разі потреби. Це повинно регулюватися системою.

Система повинна бути досить простою. У той час як зручність використання може ніколи не поставити під загрозу безпеку, це може зробити складність системи. Отже, співвідношення рівня безпеки та рівня складності системи повинно бути збалансованим. Зокрема, це стосується зручності використання, архітектури системи і можливих інтеграцій. Робота зі складною системою призводить до занадто багатьох залежностей, які ставлять під загрозу безпеку.

Місія системи безпеки повинна бути захищена від атаки, а не окремі компоненти системи. Тобто система в цілому повинна бути захищеною, а не кожен окремий її компонент.

Для того щоб допомогти у виборі і реалізації рішень у сфері безпеки, принципи безпеки повинні бути оцінені, інтерпретовані і застосовані для вирішення конкретного завдання. За допомогою оцінки та інтерпретації кожного принципу виявляються багато загроз для системи безпеки, в результаті чого може бути визначений перелік вимог до захисту. Метою є отримання повного набору параметрів, необхідних для забезпечення безпеки. Слід зазначити, що даний набір параметрів, специфічний для конкретного завдання яке необхідно вирішити, також називається «завданням безпеки».

Аналізуючи питання з позиції виробника, ми з'ясували, що сфера використання принципів безпеки не повинна обмежуватися процесами вибору і впровадження продукту, оскільки дані принципи застосовні протягом усього життєвого циклу розробки продукту. Наше завдання полягає в тому, щоб забезпечити клієнтам реалізацію заходів безпеки, які відповідають їхнім побажанням і вимогам, а також місцевим законам і обмеженням бюджету. Виходячи з цього, ми виробили принципи безпеки, щоб дозволити нашим клієнтам реалізувати їх головну мету створити безпечне оточення, а також виявляти і відстежувати всіх людей, які входять в їх компанію.

Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашифрованих повідомлень практично неможливо.

Потужним та дієвим є застосування для захисту інформації систем, що дозволяють шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того,

що для шифрування та дешифрування використовувався один і той же секретний ключ, який мав мати відправник і отримувач повідомлення. Одним з поширених, сьогодні, методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, що не є секретним з допомогою якого проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) - це аналог власного підпису посадової особи в електронному вигляді.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регулювальників безпеки, є основою реалізації багатьох з них і, в той же час, останнім захисним рубежем.

Актуальність цих проблем підкреслюється також тією обставиною, що персональний комп'ютер або автоматизоване робоче місце (АРМ) є частиною систем обробки інформації, систем колективного користування , обчислювальних мереж . У таких випадках пред'являються досить жорсткі вимоги щодо надійності та достовірності переданої інформації.

Метою захисту інформації є: запобігання витоку, розкрадання, втрати, перекручування, підробки інформації; запобігання загрозам безпеки особистості, суспільства, держави; запобігання несанкціонованих дій по знищенню,системи забезпечення правового режиму документованої інформації як об'єкта власності; захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, що є в інформаційних системах; збереження державної таємниці, конфіденційності документованої інформації відповідно до законодавства, забезпечення прав суб'єктів в інформаційних процесах при розробці, виробництві та застосуванні інформаційних систем, технологій та засобів їх забезпечення .

Завдання захисту інформації в інформаційних обчислювальних системах вирішується , як правило, досить просто: забезпечуються засоби контролю за виконанням

програм, що мають доступ до збереженої в системі інформації. Проте при широкому поширенні обчислювальних та інформаційних систем, особливо в таких сферах, як обслуговування населення ,банківська справа, цих заходів виявилося явно недостатньо.

Система, що забезпечує захист інформації, не повинна дозволяти доступу до даних користувачам, які не мають такого права. Така система захисту є невід'ємною частиною будь-якої системи колективного користування засобами обчислювальної техніки, незалежно від того, де вони використовуються.

Органи державної влади та організації, відповідальні за формування та використання інформаційних ресурсів, що підлягають захисту, а також органи та організації, що розробляють та застосовують інформаційні системи та технології для формування та використання інформаційних ресурсів зобмеженим доступом, керуються в своїй діяльності законодавством України.

Контроль за дотриманням вимог до захисту інформації та експлуатації спеціальних програмно-технічних засобів захисту, а також забезпечення організаційних заходів з захисту інформаційних систем, що опрацьовують інформацію з обмеженим доступом в недержавних структурах, здійснюються органами державної влади. Організації, які опрацьовують інформацію з обмеженим доступом, що є власністю держави, створюють спеціальні служби для забезпечення захисту інформації.

Великою проблемою для постачальників продуктів у сфері управління системами безпеки є те, що їм доводиться пропонувати рішення, які повинні відповідати багатьом, іноді суперечливим вимогам клієнтів. Необхідність в комерційних, готових продуктах для управління системами безпеки змушує постачальників впроваджувати багатофункціональні, гнучкі, зручні у використанні і легко адаптивні продукти, які можуть вирішувати широкий спектр завдань безпеки і повинні відповідати принципам безпеки в такому вигляді, в якому їх оцінив, інтерпретував і застосував клієнт. Єдиний спосіб досягти цього надавати продукти, які мають широкі можливості конфігураціїі адаптації.

Література:

1. World Vision in principles of network security, scientific and informative article. URL:https://worldvision.com.ua/ua/articles/printsipi-bezopasnosti (дата звернення: 14.02.2021)

2. Infopedia in principles of network security. URL: https://infopedia.su/1x2f0c.html (датазвернення: 14.02.2021)

РОЗРОБЛЕННЯ ВЕБ-ДОДАТКУ «ВСЕУКРАЇНСЬКИЙ ІСТОРИЧНИЙ ПЛЕНЕР «ХАРКІВ КРІЗЬ ВІКИ»»

Носань Юрій Володимирович
Харківський національний економічний університет ім. Семена Кузнеця
м. Харків

Використання веб-додатків (веб-сайтів) для позповсюдження інформації - це досить простий і популярний метод, тому ця форма реалізації даного проекту є актуальною.

Метою проекту було створення доступного місця для перегляду робіт художників, що брали участь в пленерах, проведених з ініціативи університету. Студенти університету, а також будь-які інші гості веб-сайту, зможуть подивитися на картини, які були написані. Після проведення кількох пленерів потрібно було зняти деякі картини зі стін університету, але їх доступність не змінилася. Також даний проект підтримує початкову мету проведення пленерів, а саме залучення до творчого мислення та свого роду культуризацію студентів.

Критерії оцінки здібностей фахівців невпинно змінюються. Компетентність, ерудованість були й залишаються суттєвими професійними якостями фахівця, але в умовах прискоренного науково-технічного прогресу та ускладнених технічно-інформаційних процесів цього може не вистачити. [1, 64]

Важливо розуміти що, необхідне виховання і самовиховання високої методологічної культури мислення, здібності не лише орієнтуватися на потоках професійної та ідейно-політичної інформації, але й правильно її обробляти, вміти самому шукати нові знання. Соціалізація молодої людини охоплює всі сфери її життєдіяльності, впливає на більшість аспектів їх життя, і цей вплив має двосторонній характер, тобто обраний спосіб життя та самого методу соціалізації впливає на подальше формування соціально-активної, гармонійно розвинутої особистості, або інших менш популярих типів. Зростання освітнього рівня молоді не призводить автоматично до підвищення мотивації задоволення культурних потреб. Культура, як засіб соціалізації молоді, контролює, регулює, впорядковує поведінку суб'єктів соціальної взаємодії. Її не можна засвоїти безпосередньо у колективно організованих формах дозвілля. У процесії еволюції було сформовано цілу мережу культурно-освітніх закладів: школи, театри, кінотеатри, ЗМІ та комунікації, заклади агітації й пропаганди, просвітницькі

установи, церква, музеї тощо. Стосовно окремої особи культура, як ресурс розвитку, сприяє формуванню духовних якостей особистості. [2, 243]

Слово ректора

«У Харкові 22 – 31 липня 2019 року з великим успіхом пройшов Всеукраїнський історичний пленер «Харків крізь віки». За збігом обставин захід вирішили провести саме цього року, до 175-річчя від дня народження великого живописця Іллі Юхимовича Репіна, нашого славетного земляка.

Пленер було присвячено нобелівському лауреату Семену Кузнецю, який у 1919–1922 роках навчався у Харківському комерційному інституті, а сьогодні його альма-матер, Харківському національному економічному університету, присвоєно ім'я цього видатного вченого. Тому природним є те, що на базі університету було вирішено провести цей пленер. До того ж, науково-педагогічна та студентська спільнота нашого університету вважає за аксіому, що підготувати справжнього професіонала своєї справи світового рівня неможливо без виховання мистецтвом, яке охоплює собою художнє оточення і діє іноді непомітно, але повсякденно і повсякчасно.

Ми розглядаємо мистецтво як засіб духовного освоєння людиною дійсності, формування її здатності за допомогою своєї творчості перетворювати навколишній світ згідно із законами гармонії, що втілюються у живопису, музиці, літературі, архітектурі тощо. Надзвичайної важливості цьому заходу надала участь поважного гостя, народного художника України, лауреата Шевченківської премії, голови ХО НСХУ України Віктора Івановича Ковтуна та заслуженого діяча мистецтв України, члена НСХУ Володимира Анатолійовича Носаня.

Науково-педагогічна та студентська спільнота висловлює велику вдячність учасникам заходу за роботи, які вони від щирого серця подарували для галереї нашого університету.»

В. С. Пономаренко,
Ректор ХНЕУ ім. С. Кузнеця,
заслужений діяч науки і техніки України,
лауреат Державної премії в галузі науки і техніки України,
член-кореспондент Національної академії педагогічних наук України

Література:

1. Выготский Л. С. Педагогическая психология. - Москва, 1996.

2. Левин В. А. Воспитание творчества. - М.: Знание, 1977.

ОПТИМІЗАЦІЯ МЕРЕЖІ ІНТЕРНЕТ РЕЧЕЙ

Огіренко Ярослав Вадимович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Оптимізація мережі - одна з головних проблем, з якою стикається IoT найближчі роки. У цій роботі представлені підходи, пов'язані з оптимізацією мережі для зв'язку IoT. Різні типи алгоритмів для багатоцільових задач, енергія QoS ефективні кооперативні кластери, ієрархічні сенсорні мережі, підходи для оптимізації енергоефективності в Інтернеті речей та безпечний енергоефективний протокол маршрутизації.

Спочатку Інтернет використовувався для передачі пакетів даних між користувачами та джерелами даних з певною IP-адресою [1]. Завдяки вдосконаленням, Інтернет використовується для обміну даними між різними невеликими пристроями з обмеженими ресурсами, які утворюють Інтернет речей (IoT). IoT забезпечує взаємозв'язок мільярдів датчиків, виконавчих механізмів, навіть людей з Інтернетом, створюючи широкий спектр послуг, деякі з яких критично важливі. Велика кількість даних з цих пристроїв накладає витрати на мережу IoT. Однак мережі IoT мають недоліки: речі обмежені ресурсами з точки зору енергії та обчислювальних можливостей. Отже, для забезпечення оптимального використання наявної мережі потрібно забезпечити рішення для різноманітних проблем, пов'язаних з мережею IoT, включаючи маршрутизацію, енергозбереження, неоднорідність, масштабованість, надійність, якість обслуговування (QoS) та безпеку. У цій роботі представлено огляд щодо оптимізації мережі Інтернет речей.

Для систем IoT, що виконують критичну місію, надзвичайно важливо забезпечити зв’язок, доступність та надійність мережі, що вимагає активного моніторингу мережі. Ідея полягає у нагляді за станом мережі та функціонуванням вузлів та додатків для забезпечення раннього виявлення несправностей та зменшення часу недосяжності вузла. Обов’язково мінімізувати споживання енергії, щоб мережа IoT могла виконувати свою основну функцію [2]. У цьому складному контексті першим кроком аналізу є забезпечення (оптимального) розміщення моніторингових вузлів (моніторів), які охоплюють даний домен.

Як правило, оптимізація мережі визначається як технологія і використовується для підвищення продуктивності мережі для будь-якого навколишнього середовища. Це відіграє важливу роль в IT, оскільки день за днем кількість даних із різних типів пристроїв та програм заповнюється в мережі. Пропозиції щодо оптимізації мережі має різні переваги, такі як

висока швидкість передачі даних, відновлення даних, усунення надлишкових даних та збільшення часу відгуку програми та мережі.

Оптимізація мережі в Інтернеті речей привертає все більшу увагу до очікування високого збільшення трафіку від речей IoT та об'єктів, оскільки мільярди пристроїв IoT, як очікується, підключатимуться у глобальні мережі в найближчі роки [3,4]. Завдяки цьому очевидно, що дослідники та оператори можуть запропонувати ефективне рішення для оптимізації мереж IoT для зменшення трафіку, створюваного IoT, що впливає на інші послуги в мережі та ефективно використовувати мережеві ресурси. Трафік, що генерується пристроями IoT, відрізняється від стільникової мережі через неоднорідність програм та типів пристроїв. Крім того, потік IoT потрібно регулювати, щоб контролювати роботу IoT пристроїв та його послуг. Результат цієї роботи підкреслює важливість оптимізації мережі Інтернету речей.

Література:

1. https://www.sciencedirect.com/science/article/pii/S2215098618303379

2. S. Li, L. Da Xu, S. Zhao, The internet of things: a survey, Inf. Syst. Front. 17 (2) (2015) 243–259.

3. L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Networks 54 (15) (2010) 2787–2805.

4. J. Francois, T. Cholez, T. Engel, CCN Traffic optimization for IoT, in Fourth International Conference on the Network of the Future (NoF), 2013, pp. 1–5.

INTERNET OF THINGS: CHALLENGES AND SOLUTIONS

Nikita Ozhyhin
State University of Telecommunications
Institute of Informational Technologies
Kyiv

For the last few years a new technology has been rising and growing quickly. This technology is called Internet of Things (further – IoT). IoT has seen a visible growth as more businesses look to maximize connectivity and data to drive efficiency, automate critical operations and elevate visibility over their assets. However, both, users and developers, can come across difficulties emerged by using these types of systems.

Everyone reading this will be aware of the explosive growth of sensors and devices that communicate—that is, the Internet of Things (IoT). The IoT now covers virtually every aspect of human interest and existence. These IoTs are within our bodies, on our bodies, observing our activities, monitoring and reporting on our appliances, houses, and buildings, our cars and environment, and many facets of our cities, planet, oceans, and space. They are starting to play a role in our health, fitness and wellbeing, our

comfort and entertainment, our financial activities, and many other facets of life.

First of all, there are some interoperability and middleware challenges in order to achieve interoperability at the device, networking, and data-exchange levels. We are able to cope with these issues relying on our past experiences with similar challenges. For instance, we have Samsung and Google's cooperation on a low-power wireless network called Thread (https://www.threadgroup.org/). It uses Bluetooth Smart to enable connection between devices. Also, we have Samsung, Dell, and Intel's efforts on the Open Interconnect Consortium. Their aim is to create a system that will be able to connect any device with another, regardless of all the differences that can be present in given gadgets. However, interoperation and data integration issue is more important and demanding task. To achieve the given purpose, one technology, called Semantic Gateway as Service (SGS), [1] allows to translate between a wide range of IoT messaging protocols in nowadays use, such as the Extensible Messaging and Presence Protocol (XMPP), the Constrained Application Protocol (CoAP), and MQTT. Another important interoperability capability is provided by the World Wide Web Consortium (W3C)'s Semantic Sensor Network (SSN) ontology and annotation framework. [2]

The recipients of all this data will face an even bigger challenge. Firstly, how is it possible for all this information to find its way to those who can manage it and use it properly? Secondly, how big data overloads can be foreseen, prevented and coped with in time?

The solution is obvious, yet hard to implement: we need highly contextualized and personalized data that's also manageable, so called "smart data".

As our ability to create smart data advances, we will see more abilities on the part of machines to intelligently filter just the data that's needed to meet its human master's needs, assimilate all forms of contextually relevant data, personalize it by factoring in a user's preferences and needs, and present the results at a level of abstraction that's ready for a human to act on. [3]

References:

1. P. Desai, A. Sheth, and P. Anantharam, "Semantic Gateway as a Service Architecture for IoT Interoperability", 18 Oct. 2014 (http://xxx.tau.ac.il/abs/1410.4977)

2. M. Compton et. al., "The SSN Ontology of the W3C Semantic Sensor Network Incubator Group", Dec.2012, doi:10.1016/j.websem.2012.05.003

3. Amit Sheth, Kno.e.sis Center, Wright State University "Internet of Things Perspectives"

ПРОЦЕСАМИ ЗАВДЯКИ ПЛАТФОРМАМ RPA-ТЕХНОЛОГІЙ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

Ольховський Максим Олегович, Пінчук Дар'я Валеріївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Не секрет, що значна кількість великих компаній на світовому ринку вже налаштували автоматизацію своїх бізнес-процесів. Основні причини зрозумілі: зниження витрат (у тому числі на зарплату співробітникам, соцпакет і вихідну допомогу) та підвищення ефективності. Для цього в світі все частіше почали застосовувати RPA-технології.

RPA – це набір певних технологій, призначених для автоматизації рутини в роботі офісних співробітників. Здатні автоматизувати прискорення введення даних в різні аналітичні системи котрі використовує компанія, виконання простих шаблонних дій в обліковому записі та інші операції які можна виконати притримуючись алгоритму, без участі людини. Іншими словами, це заміна людини спеціально створеним ботом що вибирає свої наступні дії через програмований алгоритм. Однак, на відміну від макросу, який просто робить чітко заданий порядок справ, цей бот навчається за рахунок машинного навчання (Machine Learning, ML). Такий бот може самостійно приймати рішення як діяти далі в залежності від певної ситуації.

Штучний інтелект (Artificial intelligence, AI) – різноманітні технологічні та наукові рішення і методи, які допомагають розроблювати програми які будуть здатні уподібнюватися інтелекту людини. Artificial intelligence охоплює безліч інструментів, алгоритмів і систем, серед яких також усі складові Data science і Machine learning.

RPA належить до так званих low-code систем, це означає, що її набагато легше впровадити в уже існуючу систему підприємства. Їхня структура така, що немає необхідності перебудовувати вже існуючі процеси і системи у компанії. Бо RPA-технології підлаштовуються під них, а не навпаки. Належність RPA-технологій до low-code систем, означає що для створення потрібних рішень роботи системи використовуються вже готові модулі. В результаті цього розробка софта відбувається при мінімальному використанні ручного набору коду і максимальній автоматизації завдань.

Великим плюсом такого підходу є можливість ефективно працювати з RPA-технологіями навіть молодим фахівцям з невеликим досвідом в програмуванні. У той же час програмісти вищого рівня можуть переключитися на більш складні і творчі завдання.

На сьогодні існує уже достатня кількість RPA-рішень з використанням штучного інтелекту для різних сфер бізнесу. Кожне з них вирішує власні завдання характерні для своєї ніші бізнесу, значно полегшує щоденну рутину співробітників і прискорює вирішення бізнес-задач.

Одна з таких - це платформа WorkFusion – готове рішення для автоматизації всіх бізнес-процесів на базі штучного інтелекту. В платформу інтегровані боти, які навчаються в режимі реального часу і швидко адаптуються під автоматичні процеси підприємства. Платформа позиціонує себе як ідеальне рішення для банків, страхових компаній і системи охорони здоров'я.

WorkFusion використовує Standart Bank, найбільший банк Африки, з капіталізацією більше 164 мільярдів доларів, 10 мільйонами клієнтів і сотнею тисяч співробітників. Банк перейшов на використання WorkFusion, щоб відповідати очікуванням клієнтів, які в сучасному цифровому світі вимагають швидких результатів 24/7. На додачу до цієї мети банку також вдалося знизити витрати і прискорити своє зростання.

Ще один приклад – існуюча платформа Hyperscience, це комп'ютерний зір для обробки і розпізнавання документів англійською мовою. Система переводить дані з документації англійською мовою - як друкованої, так і написаної від руки, в електронний вигляд. Вона сама визначає тип контенту за допомогою штучного інтелекту і витягує дані для подальшої обробки. І звільняє при цьому більше 80% часу, який зазвичай витрачається на сортування документів вручну, введення даних. Також система спрощує навігацію по всіх документах компанії, до яких надано доступ, враховує стандартні випадки і винятки з правил.

Hyperscience також допомагає складати звіти більш ефективно, враховуючи навіть ті дані, які користувач-людина може не врахувати. Завдяки штучному інтелектові, що лежить в її основі, система автоматично сортує всі нові документи і постійно навчається для більш ефективної роботи з ними.

Література:

1. *https://evergreens.com.ua/ua/articles/review-rpa.html*
2. *https://www.uipath.com/rpa/robotic-process-automation*
3. *https://www.workfusion.com*

СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ ТА НЕЙРОННІ СИСТЕМИ. МЕРЕЖІ LSTM

Ольховський Максим Олегович, Пінчук Дар'я Валеріївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Машинне навчання - це клас методик, який можна використовувати для аналізу даних або інформації з метою узагальнення та дотримання шаблонів цих даних чи інформації. Для прогнозування майбутньої цінності чи поведінки з цих спостережень чи зразків вона буде ітеративно вчитися на даних, на відміну від типових комп'ютерних програм. Мета машинного навчання - запрограмувати комп'ютери на використання зразкових даних у якості минулий досвід чи модель, і використовувати шаблони цих даних для прогнозування майбутнього на основі цих даних.

Нейронні мережі - це штучно навчені мережі, мета яких є спробою моделювання здатності людського мислення, зокрема, здатності навчатися і вирішувати задачі розпізнавання по прецедентах. Вони засновані на досягненнях біології і медицини — найпростіших моделях людського мозку, створених у середині минулого століття.

Штучні нейронні мережі надзвичайно різноманітні за конфігураціями. Незважаючи на це, мережеві парадигми мають багато спільного. Нейронні мережі розрізняють за топологічними типами відповідно до структури звязків між нейронами мережі, а також за типом використаних формальних нейронів.

ШНМ можуть розглядатися як спрямований граф зі зваженими зв'язками, у якому штучні нейрони є вузлами. По архітектурі зв'язків ШНМ можуть бути згруповані в два класи: мережі прямого поширення, у яких графи не мають петель, і рекурентні мережі, або мережі зі зворотними зв'язками.

Довга короткострокова пам'ять (Long short-term memory; LSTM) - особливий різновид архітектури рекурентних нейронних мереж, здатна до навчання довготривалим залежностям. Вони були представлені Зеппом Хохрайтер і Юргеном Шмідхубер (Jürgen Schmidhuber) в 1997 році, а потім вдосконалені і популярно викладені в роботах багатьох інших дослідників. Вони прекрасно вирішують цілий ряд різноманітних завдань і в даний час широко використовуються.

LSTM розроблені спеціально, щоб уникнути проблеми довготривалої залежності. Запам'ятовування інформації на довгі періоди часу - це їх звичайна поведінка, а не щось, чого вони насилу намагаються навчитися.

Будь-яка рекуррентная нейронна мережа має форму ланцюжка повторюваних модулів нейронної мережі. У звичайній RNN структура одного такого модуля дуже проста,

наприклад, він може являти собою один шар з функцією активації tanh.

Не всі LSTM однакові. Взагалі, здається, що в кожній новій роботі, присвяченій LSTM, використовується своя версія LSTM. Відмінності між ними незначні, але про деякі з них варто згадати.

Одна з популярних варіацій LSTM, запропонована Герсом і Шмідхубером (Gers & Schmidhuber, 2000), характеризується додаванням так званих «оглядових вічок» («peephole connections»). З їх допомогою шари фільтрів можуть бачити стан осередку.

Інші модифікації включають об'єднані фільтри «забування» і вхідні фільтри. У цьому випадку рішення, яку інформацію слід забути, а яку запам'ятати, приймаються не окремо, а спільно. Ми забуваємо будь-яку інформацію тільки тоді, коли необхідно записати щось на її місце. Ми додаємо нову інформацію з стан осередку тільки тоді, коли забуваємо стару.

Трохи більше відрізняються від стандартних LSTM керовані рекурентні нейрони (Gated recurrent units, GRU), вперше описані в роботі Cho, et al (2012). У ній фільтри «забування» і входу об'єднують в один фільтр «оновлення» (update gate). Крім того, стан комірки об'єднується з прихованим станом, є й інші невеликі зміни. Побудована в результаті модель простіше, ніж стандартну LSTM, і популярність цієї моделі неухильно зростає.

У даній роботі ми розглянули лише кілька найбільш примітних варіацій LSTM. Існує безліч інших модифікацій, як, наприклад, глибокі керовані рекурентні нейронні мережі (Depth Gated RNNs), представлені в роботі Yao, et al (2015). Є й інші способи вирішення проблеми довгострокових залежностей, наприклад, Clockwork RNN Яна Кутніка (Koutnik, et al., 2014 року).

Отже, LSTM-мережі - значний крок у розвитку рекурентних нейронних мереж. Їх використання дозволяє уникнути проблеми довготривалих залежностей, розширюючи коло завдань, що вирішуються за допомогою методів машинного навчання. LSTM-мережі зайняли своє місце серед інших штучних нейронних мереж, ставши найбільш популярним рішенням в сфері обробки природної мови.

Література:

1. *http://om.univ.kiev.ua/users_upload/15/upload/file/pr_lecture_10.pdf*
2. *https://pidru4niki.com/12291025/informatika/neyromerezhevi_tehnologiyi_shtuchnogo_intelektu*
3. *https://ela.kpi.ua/bitstream/123456789/32011/1/Bukhanenko_magistr.docx*

ВИКОРИСТАННЯ ПРОТОКОЛУ Z-WAVE ДЛЯ ПОБУДОВИ СИСТЕМИ РОЗУМНОГО БУДИНКУ АБО ОФІСУ

Онучин Микита Романович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Дослідження протоколу Z-Wave для розумних систем, його використання та переваги над іншими протоколами.

Що таке Z-Wave?

Z-Wave - це запатентований бездротовий протокол. Його розробили для домашньої автоматизації, в основному для контролю і управління в житлових і комерційних об'єктах. Цю технологію використовують в побутовій електроніці і різних приладах для опалення, освітлення або для контролю доступу. В прилади вбудовують радіочастотні модулі.

Z-Wave - це бездротова радіо технологія з низьким енергоспоживанням. ЇЇ розробили для керування пристроями дистанційно. Z-Wave працює в діапазоні частот до 1 ГГц і дуже добре оптимізована та має малі затримки для передачі керуючих команд, в той час як Wi-Fi і інші IEEE 802.11 стандарти призначені для великого об’єму даних.

Різновид протоколів, використання, переваги та недоліки

Z-Wave призначений для створення недорогої та енергоефективної електроніки. До них можна віднести пристрої на батарейках. А до цих пристроїв відносяться пульти дистанційного керування, руху та інших види та типи датчиків.

У 2013 році компанія Sigma Designs, власник технології Z-Wave, представила розширення протоколу Z-Wave з новою назвою Z-Wave Plus.

Z-Wave Plus це стандартний протокол Z-Wave, але з доповненим списком вимог, який відрізняється від звичайних вимог сертифікації Z-Wave. Тобто у Z-Wave Plus є всі ті вимоги що і у Z-Wave, але ще й і нові, які створили для покращення взаємодії між різними пристроями які є на ринку.

Цей протокол має багато плюсів:

а) Більше ніж 4 млрд зашифрованих кодів безпеки для запобігання клонування;

б) Надійний мережевий протокол;

в) Можливість віддаленого моніторингу;

г) Не потребує прокладання нових кабелів;

д) Простий у модернізації та розширенні за допомогою додавання нових пристроїв в будь-який момент;

е) Підтримка сумісності з пристроями виготовленими різними виробниками у яких є логотип Z-Wave.

Але є і мінуси у цієї технології. Наприклад через низьку швидкість передачі даних не можливо передавати зображення або звук.

Інколи для рішень з понад 30 пристроїв, технологія Z-Wave програє по вартості, ніж кабельні системи.

Не завжди може вистачити радіуса дії і тому необхідно використовувати повторювачі або кабелі.

Переваги над іншими протоколами

Порівнявши Z-Wave з іншими протоколами можна сказати, що цей протокол має перевагу над іншими у тому, що працює по бездротовій мережі та використовую частоту до 1 ГГц, тому перебоїв через інші бездротові мережі не буде. Також ще однією перевагою розумної системи на протоколі Z-Wave є те, що не обов'язково потрібен вихід у глобальну мережу Інтернет. Також обладнання для побудови розумної системи по вартості буде меншою ніж у інших протоколів, бо кількість та різноманітність дуже багата.

Висновок

Протокол Z-Wave – це хороший, ефективний варіант для побудови розумної системи. У поєднані з низькою вартістю обладнання та великим вибором, а також роботи на частотах до 1ГГц, без обов'язкового підключення до інтернету, можна побудувати високоякісну розумну систему.

Література:

1. Андрей Дементьев, «Умный дом XXI века», 2016. 43 с.

2. ПРОТОКОЛ 1-WIRE URL: http://avr.ru/beginer/understand/1wire

ТЕХНОЛОГІЇ СИСТЕМ РОЗУМНОГО БУДИНКУ ТА ОФІСУ

Онучин Микита Романович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

У даній статті розглядається питання технологій для розумних систем, їх використання, переваги та недоліки. Розумні системи все частіше починають використовувати у різних сферах. Хтось автоматизує будинок для комфортного перебування в ньому, хтось автоматизує офіс, для енергоефективності та кращих умов праці для працівників.

У статті розглянуться існуючі технології на ринку та їх характеристики.

Вступ

На сьогоднішній день вже дуже багато «розумних» будинків та офісів створено. Їх створюють для того, щоб людині було комфортно, безпечно та простіше жити або працювати. Але інколи для покращення необхідно витратити мінімум затрат, тому потрібно дослідити можливі технології для визначення найкращої для конкретних цілей.

Основна частина

Технологія x10. Один з перших протоколів які з'явилися ще в 70-х роках минулого століття – це x10. Цей стандарт є відкритим. Він використовує в якості середовища передачі силову електропроводку і тому прокладати додаткові кабелі не потрібно для пристроїв, які працюють з цим стандартом.

Для роботи бездротових пультів, перемикачів та інших пристроїв був розроблений протокол використання радіоканалу. Бездротові пристрої передають по радіоканалу пакети даних, а для передачі використовується частота 310 МГц в США і 433 МГц в Європі.

Але цей протокол був створений давно, тому має ряд суттєвих недоліків. Цей протокол досить повільний, для передачі адреси та команди може зайняти 3/4 секунди. Інші більш сучасніші протоколи працюють швидше. Також у мережі X10 можна передавати тільки одну команда та в конкретний момент часу, якщо в один і той же час буде йти передача більше ніж однієї команди, то це призведе до колізії. Колізія – це коли команда не буде правильно прийнята або будуть виконані неправильні дії.

Технологія KNX. KNX - це відкритий стандарт для автоматизації комерційних та побутових будівель.

Протокол KNX можна переглянути, ґрунтуючись на мережевій моделі OSI. Це децентралізована однорангова мережа з керуванням подіями. Мережа KNX підтримує стандартний протокол передачі даних, який реалізований у різних середовищах передачі:

а) кабель із крученою парою;

б) лінія електропередачі;

в) Мережа IP (EIB.net);

г) радіоканал.

Передача здійснюється модуляцією напруги в мережі, а логічний нуль надсилається як імпульс, з амплітудою приблизно ± 6 В. Відсутність імпульсу інтерпретується як логічна одиниця. Інформація надсилається пакетами з 8 байтів. Переадресація синхронізується з бітами запуску та зупинки. Також є біт контролю парності.

Для вирішення зіткнень інформації в мережі використовується метод CSMA / CA. Цей метод гарантує випадковий, безперебійний доступ пристроїв до шини, без істотного зниження його максимальної пропускної здатності. Повідомлення з найвищим пріоритетом будуть передані в першу чергу.

KNX розвинувся за трьома попередніми стандартами: Європейський протокол домашніх систем (EHS), BatiBUS та європейська інсталяційна шина (EIB або Instabus). Він може використовувати виту пару (в топології дерева, лінії чи зірки), лінії електропередач або IP.

Технологія ZigBee. Zigbee - це специфікація на базі IEEE 802.15.4 для набору протоколів зв'язку високого рівня, що використовуються для створення персональних мереж з невеликими цифровими радіоприймачами. Zigbee використовують для домашньої автоматизації, збору даних з медичних пристроїв та інших проектів яким необхідний бездротовий зв’язок та використання не потужних та з низькою пропускною здатністю пристрої.

Технологія Zigbee простіша і дешевша, ніж інші бездротові персональні мережі, такі як Bluetooth або більш загальні бездротові мережі, такі як Wi-Fi.

Через низьке споживання електроенергії є певні обмеження у відстані для передачі даних. Але пристрої Zigbee можуть передавати дані і на великі відстані, використовуючи різні проміжні пристрої, які допоможуть збільшити дальність передачі даних. Zigbee зазвичай використовують для задач із низькою швидкістю передачі даних, тривалого часу роботи акумулятора та безпечної мережі. Мережі Zigbee захищені 128-бітовими симетричними ключами шифрування. Zigbee має швидкість 250 кбіт / с та найкраще підходить для періодичної передачі даних від датчика або від пристроя вводу.

Назвали цю технологію так, через схожу поведінку бджіл, які повертаються у вулик.

У цієї технології є ряд переваг:

а) специфікація ZigBee має криптографічний захист даних, а також має гнучку політику безпеки;

б) мережа ZigBee є самовідновленною і гарантує доставку пакетів у разі втрати зв'язку між вузлами, перезавантаженням або відмови якогось елементу;

в) пристрої ZigBee мають низьке електроспоживання;

г) пристрої ZigBee невеликі за розміром та коштують не дуже дорого.

Технологія Z-Wave. Z-Wave - це запатентований бездротовий протокол. Його розробили для домашньої автоматизації, в основному для контролю і управління в житлових і комерційних об'єктах. Цю технологію використовують в побутовій електроніці і різних приладах для опалення, освітлення або для контролю доступу. В прилади вбудовують радіочастотні модулі.

Z-Wave - це бездротова радіо технологія з низьким енергоспоживанням. ЇЇ розробили для керування пристроями дистанційно. Z-Wave працює в діапазоні частот до 1 ГГц і дуже добре оптимізована та має малі затримки для передачі керуючих команд, в той час як Wi-Fi і інші IEEE 802.11 стандарти призначені для великого об’єму даних.

Z-Wave призначений для створення недорогої та енергоефективної електроніки. До них можна віднести пристрої на батарейках. А до цих пристроїв відносяться пульти дистанційного керування, руху та інших види та типи датчиків.

Цей протокол має багато плюсів:

а) Більше ніж 4 млрд зашифрованих кодів безпеки для запобігання клонування;

б) Надійний мережевий протокол;

в) Можливість віддаленого моніторингу;

г) Не потребує прокладання нових кабелів;

д) Простий у модернізації та розширенні за допомогою додавання нових пристроїв в будь-який момент;

е) Підтримка сумісності з пристроями виготовленими різними виробниками у яких є логотип Z-Wave.

Але є і мінуси у цієї технології. Наприклад через низьку швидкість передачі даних не можливо передавати зображення або звук.

Інколи для рішень з понад 30 пристроїв, технологія Z-Wave програє по вартості, ніж кабельні системи.

Не завжди може вистачити радіуса дії і тому необхідно використовувати повторювачі або кабелі.

Технологія 1-Wire. 1-Wire - протокол передачі даних, який працює в обидві сторони та використовуючи однин дріт.

Даний протокол розроблений корпорацією Dallas Semiconductor (зараз Maxim Integrated) в далеких 90-х роках. Зараз він активно використовується у більшості домофонних чіпів, карток доступу, а також завдяки 1-Wire спілкуються датчики температури, транзисторні ключі, програмовані порти введення-виведення і багато іншого обладнання.

Режим зв'язку в цьому протоколі - асинхронний і напівдуплексний, а також "гострий". У цьому режимі

надсилаються мультибайтні дані і передача йде від молодшого байта до старшого.

На шині має бути лише один пристрій, який відсилатиме команди. Також до загальної шини підключаються пристрої, які приймають команди і відповідають на них.

Протокол 1-Wire хороший тим, що не складний в реалізації і для зв'язку потрібно всього два або три дроти. Це шина даних, земля і живлення. Але у цьому протоколі є і недоліки - він досить чутливий до часу та перешкод. Також 1-Wire не здатен передавати великий обсяг даних та не має високої швидкості обміну даними.

Використовується 1-Wire у пристроях для ідентифікації та авторизації. Наприклад у ключах та картках пропуску. Також і у багато яких датчиках. Наприклад датчики температури або вологості, освітлення та інші датчики.

До переваг можна віднести:

а) для зв'язку з пристроєм потрібно лише два дроти - дані і заземлення, але інколи потрібен третій дріт живлення;

б) у процесі роботи мережі можна змінити конфігурацію;

в) велика відстань передачі даних.

Технологія Bluetooth Low Energy (BLE). У 1999 році з'явилася нова стандартна технологія бездротового зв'язку, яку назвали Bluetooth. Протягом багатьох років ця технологія розвивалась, для того щоб вона з’явилася в пристроях, які ми використовуємо кожного дня. Лише через десять років з'явився Bluetooth Low Energy (BLE) з версією 4.0. У цієї версії такі ж самі функції, як і у того Bluetooth, що був створений раніше, але він більше оптимізований та зменшили споживання енергії.

Головною перевагою Bluetooth Low Energy є його дуже низьке споживання енергії. Ця технологія в основному використовується для періодичної передачі даних у невеликій кількості та не дуже далеку дистанцію. В основному Bluetooth Low Energy споживає в двічі менше ніж Bluetooth. Також BLE залишається економічно вигіднішим при значному терміні служби акумулятора.

Bluetooth Low Energy (BLE) - це технологія, яка дозволяє швидко передавати дані з низьким споживанням. Наприклад температуру, вологість чи рух та інші. Ця технологія забезпечує вдвічі довший термін служби акумулятора, ніж звичайна технологія Bluetooth.

Недоліком можна рахувати малий вибір обладнання для побудови системи та не великий радіус дії.

Технологія Wi-Fi. Wi-Fi - назва технології бездротової мережі, яка використовує радіохвилі для забезпечення

бездротового швидкого інтернету та мережевих з'єднань. Wi-Fi - це торгова марка, яка означає IEEE 802.11x.

Бездротові мережі працюють за допомогою радіочастотної технології, частоти в електромагнітному спектрі, пов'язаної з поширенням радіохвиль. Коли на антену подається радіочастотний струм, створюється електромагнітне поле, яке потім здатне поширюватися у просторі.

Основним пристроєм бездротової мережі можна назвати точка доступу (AP).

Для того щоб пристрої могли підключитися до точки доступу та до бездротової мережі вони повинні бути обладнані адаптерами бездротової мережі.

Існує безліч технологічних стандартів для бездротових мереж. Найпоширеніші стандарти бездротових технологій включають наступні:

а) 802.11b;
б) 802.11a;
в) 802.11n;
г) 802.11ac.

Усі варіанти Wi-Fi використовують однакові радіочастоти 2,4 ГГц, і в результаті вони розроблені таким чином, щоб вони були сумісні між собою, тому зазвичай можна використовувати пристрої, засновані на різних стандартах у будь-якій бездротовій мережі.

Технологія WiFi захищена дуже добре. Як і з технологічними стандартами, методи шифрування також змінювалися. Були та є такі типи шифрування у технології WiFi:

а) WEP-шифрування;
б) TKIP-шифрування;
в) CKIP-шифрування;
г) WPA-шифрування;
д) WPA2-шифрування;
е) WPA3.

Недолік технології Wi-Fi у тому, що інші мережі будуть негативно впливати на систему, тому що працюватимуть в одному діапазоні.

Висновки

У даній статті було розглянуто особливості технологій розумних систем для будинку та офісу. Зокрема, досліджено основні технології на ринку на сьогоднішній день.

Кожна технологія має свої переваги та недоліки, тому необхідно обирати для кожної цілі потрібний протокол. Потрібно брати до уваги радіус дії, вартість, асортимент

обладнання, практичність та багато інших факторів. Завдяки розумним системам повсякденне життя буде ставити краще. Покращення може бути як у енергоефективності так і у комфорті людей у приміщенні.

Література:

1. Богданов С.В. Умный Дом. Изд. 2е, перераб. и доп. СПб.: Наука и Техника, 2005. 208 стр.

2. Андрей Дементьев, «Умный дом XXI века», 2016. 43 с.

3. Тесля Е. В. «Умный дом» своими руками. Строим интеллектуальную цифровую систему в своей квартире, 2008. 195 с.

4. Othmar Kyas. «How To Smart Home»,2017. 337c

5. Nick Vandom «Smart Homes in easy steps: Master smart technology for your home»,2018. 291c.

6. Гололобов В. Н. «Умный дом» своими руками: НТ Пресс, 2007. 416с.

7. Bluetooth Low Energy (Bluetooth LE) URL: https://internetofthingsagenda.techtarget.com/definition/Bluetooth-Low-Energy-Bluetooth-LE

8. Wi-Fi (wireless networking) URL: https://www.webopedia.com/TERM/W/Wi_Fi.html

МАШИННЕ НАВЧАННЯ

Ополончик Владислав Віталійович, Медвецький Володимир Юрійович,
В'юннік Юрій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Майбутнє вже близько і одним з доказів тому є машинне навчання. За допомогою комп`ютерних технологій та математики ми можемо до нескінченності спрощувати і прискорювати процеси, які до певного часу міг робити тільки "Homo sapiens". Розпізнавання мови, визначення хвороб, зміни погоди і не тільки. Яким чином, технологія може допомогти і автоматизувати майже всі сфери в яких задіяна людина?

Машинне навчання (Machine learning, ML) – звід методів в області штучного інтелекту, набір алгоритмів, які застосовують, щоб створити машину, яка вчиться на власному досвіді. В якості навчання машина обробляє величезні масиви вхідних даних і знаходить у них закономірності.

Не варто плутати поняття Data science і Machine learning. Ці інструменти багато в чому перетинаються, але все ж вони різні і кожен зі своїми завданнями. Також у цій статті ми раз і назавжди розберемося, як не змішувати в одну купу машинне навчання, штучний інтелект і нейромережі.

Штучний інтелект (Artificial intelligence, AI) – різні технологічні та наукові рішення і методи, які допомагають зробити програми за подобою інтелекту людини. Artificial intelligence охоплює безліч інструментів, алгоритмів і систем, серед яких також усі складові Data science і Machine learning.

Машинне навчання або Machine learning – один з розділів AI, алгоритми, що дозволяють комп'ютеру робити висновки на підставі даних, не слідуючи жорстко заданим правилами. Тобто машина може знайти закономірність у складних і багато-параметричних завданнях (які мозок людини не здатен вирішити), таким чином знаходячи більш точні відповіді. Як результат – правильне прогнозування.

Нейронна мережа за допомогою штучних нейронів моделює роботу людського мозку (нейронів), що вирішує певне завдання, самонавчається з урахуванням попереднього досвіду. І з кожним разом робить усе менше помилок. Нейромережі є одним із видів машинного навчання, а не окремим інструментом.

Першу програму на основі алгоритмів, здатних самонавчатися, розробив Артур Самуель (Arthur Samuel) в 1952 році, призначена вона була для гри в шашки. Самуель дав і перше визначення терміну «машинне навчання»: це «область досліджень розробки машин, які не є заздалегідь запрограмованими». Більш точне визначення терміну «навчання» дав набагато пізніше Т. М. Мітчелл: кажуть, що комп'ютерна програма навчається на основі досвіду E по відношенню до деякого класу задач T і заходи якості P, якщо якість вирішення завдань з T, виміряний на основі P, поліпшується з набуттям досвіду E.

Вже в 1957 році була запропонована перша модель нейронної мережі, що реалізує алгоритми машинного навчання, схожі на сучасні. В даний час ведеться розробка самих різних систем машинного навчання, призначених для використання в таких технологіях майбутнього, як Інтернет Речей, Промисловий Інтернет Речей, в концепції «розумний» місто, при створенні безпілотного транспорту і в багатьох інших.

Про те, що на машинне навчання зараз покладають великі надії, свідчать такі факти:

– в компанії Google вважають, що скоро її продукти «перестануть бути результатом традиційного програмування - в їх основу буде покладено машинне навчання»;

– компанії Google, Facebook, Apple, Amazon, Microsoft і китайська фірма Baidu вступили в боротьбу за талановитих фахівців у сфері штучного інтелекту;

– Марк Цукерберг, генеральний директор Facebook, особисто - по телефону і по відеочату - бере участь в спробах його компанії переманити найкращих випускників;

– відвідуваність на найважливіших академічних конференціях в цій сфері збільшилася майже в чотири рази.

Такі нові продукти, як Siri від Apple, M від Facebook, Echo від Amazon були створені за допомогою машинного навчання.

У найзагальнішому випадку розрізняють два типу машинного навчання: навчання по прецедентах, або індуктивне навчання, і дедуктивне навчання. Оскільки останнє прийнято відносити до області експертних систем, то терміни «машинне навчання» і «навчання по прецедентах» можна вважати синонімами. Цей метод навчання зараз, як прийнято говорити, в тренді, а ось експертні системи переживають кризу. Бази знань, що лежать в їх основі, важко узгоджувати з реляційною моделлю даних, тому промислові СУБД неможливо ефективно використовувати для наповнення баз знань експертних систем.

Навчання по прецедентах, в свою чергу, поділяють на три основних типи: контрольоване навчання, або навчання з учителем (supervised learning), неконтрольоване навчання (unsupervised learning), або навчання без учителя, і навчання з підкріпленням (reinforcement learning).

Крім названих, розробляються і інші методи навчання: активне, багатозадачне, різноманітне, трансферне і т.д. Особливо успішно розвивається в останні роки «глибоке навчання», при використанні якого можуть успішно поєднуватися алгоритми навчання з вчителем і без вчителя.

Література:

1. *https://uk.wikipedia.org/wiki/Машинне_навчання*
2. *https://habr.com/ru/hub/machine_learning/*
3. *https://www.it.ua/knowledge-base/technology-innovation/machine-learning*
4. *https://evergreens.com.ua/ua/articles/machine-learning-overview.html*

ВЕЛИКІ ДАНІ

Ополончик Владислав Віталійович,
В'юннік Юрій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Сучасна людина оточена різними гаджетами, поповнює загальну кількість "електронних даних" кожен день: збереження файлів на хмарі, музика, відео та будь-які дані які потрапляють в мережу і якими маніпулюють різні сервери. Яким чином маніпулювати даними в особливо великих масштабах? Сьогодні світ перетворився на величезний цифровий простір. Ми керуємо, ділимося та фактично зберігаємо всі аспекти нашого життя онлайн.

Дані зі всіх наших пристроїв - комп'ютерів, планшетів та смартфонів - постійно збираються та передаються в мережу, та насправді це лише початок процесу. Незабаром вся інформація буде потрапляти онлайн навіть з таких пристроїв, як годинники,

телевізори, датчики в розумних будинках, авто, обладнання на виробництві та з безлічі інших девайсів. Крім того, ми самостійно продукуємо гігабайти інформації, коли спілкуємося з друзями в соцмережах, робимо покупки онлайн, користуємося пошуком та навіть коли звантажуємо музику чи додатки.

Цікавий факт: якщо зібрати всю інформацію, яку накопичило людство з початку часів включно до 2000-го року, то виявиться, що її менше, ніж ми продукуємо зараз протягом лише одної хвилини. Цей феномен повністю змінює розуміння світу та нашого місця в ньому. Він також відомий під назвою Big Data.

Великі дані (Big Data) – позначення структурованих й неструктурованих даних величезних обсягів і значного розмаїття, що піддаються ефективній обробці програмних інструментів, які горизонтально масштабуються та з'явились у кінці 2000-х років, і альтернативних традиційних систем управління базами даних і рішенням класу рішень Business Intelligence.

Як бачимо, у цьому визначені присутні такі неоднозначні терміни, як «величезних», «значного», «ефективній» та «альтернативних». Навіть сама назва доволі суб'єктивна. Наприклад, 4 Терабайти (ємкість сучасного зовнішнього жорсткого диску для ноутбуку) – це вже великі дані чи ні? В широкому сенсі про «великі дані» говорять, як про соціально-економічний феномен, пов'язаний з появою технологічних можливостей аналізувати величезні масиви інформації, у деяких проблемних галузях – весь світовий об'єм даних, і трансформаційні наслідки, які з цього випливають.

Можна користуватись і більш простим визначенням, яке цілком відповідає усталеним і більш простим визначенням, що цілком відповідають думці журналістів і маркетологів, а саме, великі дані – це сукупність технологій, покликаних здійснювати три операції:

– обробляти більші, у порівнянні зі «стандартними» сценаріями, об'єми даних;

– уміти працювати з даними, що швидко надходять у дуже великих об'ємах. Тобто даних не просто багато, а їх постійно стає все більше й більше.

– вміти працювати зі структурованими і мало стуктурованими даними паралельно і у різних аспектах.

Вважається, що ці «вміння» дозволяють виявляти приховані закономірності, що вислизають від обмеженого людського сприйняття. Це дає безпрецедентні можливості оптимізації багатьох сфер нашого життя: державного

управління, медицини, телекомунікацій, фінансів, транспорту, виробництва і так далі. Не дивно, що журналісти і маркетологи так часто використовували словосполучення Big Data, що багато експертів вважають цей термін дикредитованим і пропонують від нього відмовитись.

Більш того, у жовтні 2015 року компанія Gartner виключила Big Data з числа популярных трендів. Своє рішення аналітики компанії пояснили тим, що до складу поняття «великі дані» входить значна кількість технологій, які вже активно застосовуються на підприємствах, вони частково стосуються інших популярних сфер і тенденцій і стали повсякденним робочим інструментом.

Раніше маркетологам доводилося вивчати своїх споживачів «вручну»: за допомогою опитувань або під час особистого спілкування. Big Data дає змогу значно автоматизувати цей процес.

Великі e-commerce компанії накопичили величезну кількість інформації про кожного з клієнтів: як часто покупець заходить на сайт, через які пристрої, де він живе, чим цікавиться, скільки покупок і коли зробив.

Таких покупців і транзакцій — мільярди, і цю інформацію в табличці Excel не обробити. На допомогу приходять фахівці (Data Scientists) і нові технології обробки даних. Коли інформація про кожного з клієнтів зібрана докупи і структурована, компанія може запропонувати своїм покупцям набагато більше. Це й вигідні для конкретного клієнта ціни, і швидке рішення проблем, і якісний сервіс. Згідно з дослідженням Capgemini Digital Transformation Institute, 81% покупців готові платити більше за кращий клієнтський досвід. Якщо персоналізований досвід клієнта настільки важливий, що люди за нього готові доплачувати, без знань про клієнта не обійтися.

Консалтингова компанія McKinsey зазначає: «Використання Big Data в банківській сфері може сприяти кращому перехресному продажу, розробці персоналізованих продуктів, динамічному ціноутворенню, кращій оцінці ризиків і більш ефективному маркетингу. А більш персоналізовані медичні послуги, крім продовження життя і поліпшення самопочуття пацієнтів, можуть заощадити від $2 до $10 трлн в усьому світі».

Такі компанії, як Netflix і Procter & Gamble, використовують Big Data для передбачення клієнтського попиту. Вони класифікують основні властивості попередніх і нинішніх продуктів, моделюють співвідношення між цими

властивостями і комерційним успіхом, і таким чином будують прогнозуючі моделі для нових продуктів і послуг.

Література:

1. *https://www.it.ua/knowledge-base/technology-innovation/big-data-bolshie-dannye*
2. *http://thefuture.news/bigdata*
3. *https://aiconference.com.ua/uk/news/tehnologii-big-data-klyuchevie-harakteristiki-osobennosti-i-preimushchestva-97883*
4. *https://content.ua/ukr/blog/big_data_pochemu_dannye_eto_novaya_neft*

РОЗВИТОК ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Осауленко Андрій Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Доповнена реальність - augmented reality або AR це середовище, що в реальному часі доповнює фізичний світ, яким ми його бачимо, цифровими даними за допомогою будь-яких пристроїв - планшетів, смартфонів або інших, і програмної частини. Нове віртуальне середовище утворюється шляхом накладання запрограмованих віртуальних об'єктів поверх відеосигналу з камери, і стає інтерактивною шляхом розпізнавання предметів середовища та використання спеціальних маркерів, тобто запрограмованих елементів, які допомагають програмі в точній взаємодії з предметами у кадрі.

Основа технології доповненої реальності - це система оптичного трекінгу. Камера розпізнає маркери в реальному світі, переносить їх у віртуальне середовище, формує зображення для виведення на екран, накладає шар цифрової інформації на реальність, і таким чином створює світ доповненої реальності.

Доповнена реальність вже багато років використовується в медицині, в рекламній галузі, в промисловій галузі, у військових технологіях та в мобільних пристроях.

Широкого розповсюдження технологія AR отримала з випуском окулярів доповненої реальності Google Glass у 2013 році. Ці окуляри мали невеликий функціонал: відображення карти з маршрутом, зйомка відео та фото шляхом голосового управління. Але саме вони представили на ринку перспективне рішення – поєднання окулярів та віртуальної реальності. Наступним схожим продуктом став Hololens – розробка компанії Microsoft. Окуляри мали вбудовані 4 камери для аналізу кімнати, високу роздільну здатність проектору, що дозволяло виводити якісне зображення на поверхню окулярів. У 2019 році було представлено друге покоління окулярів Hololens. В новій версії було збільшене поле зору в 2 рази, що дозволяє виводити удвічі більше інформації, покращене управління голограмами за допомогою жестів, також з`явилися сенсори відслідковування руху очей.

Однією із найважливіших галузей для використання AR є медицина. Наочне навчання студентів медичних університетів, де людина може бачити анімацію змін організму перед власними очима; візуалізація даних прямо на пацієнта, замість розставлених навколо екранів; УЗД стане максимально наочним, що дозволить батькам отримати на телефоні тривимірне зображення їхньої дитини.

Література:
1. *https://m.habr.com/ru/post/419437/*
2. *https://en.m.wikipedia.org/wiki/HoloLens_2*

ОГЛЯД РІШЕНЬ ІДЕНТИФІКАЦІЇ ПРИСТРОЇВ І ДОДАТКІВ ІНТЕРНЕТУ РЕЧЕЙ

Паншина Олена Леонідівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Інтернет речей є сучасною концепцією, що припускає об'єднання об'єктів, «речей», в єдину всесвітню мережу, яка дозволяє речам бути розумними для взаємодії як з один з одним, так і з людиною в будь-який час і в будь-якому місці.

На сьогоднішній день число пристроїв, підключених до мережі, перевищує число всіх жителів планети і продовжує стрімко збільшуватися, що піднімає питання про присвоєння кожному об'єкту унікальну адресу, забезпечення конфіденційності та безпеки при передачі даних. Незважаючи на це, до цих пір немає загальноприйнятого методу ідентифікації речей, який би задовольняв всім вимогам як для існуючих пристроїв і додатків Інтернету речей, так і для новостворюваних.

Ідентифікатор є виділений, публічно відомий атрибут або ім'я (або набір атрибутів та імен) для окремого пристрою. Як правило, ідентифікатори діють в межах певної області або мережі, що ускладнює ідентифікацію речей в глобальному масштабі. Зважаючи на складність і високу продуктивність сучасних пристроїв Інтернету речей вони можуть мати більше одного ідентифікатора. У той же час, існують різні методи ідентифікації, які не можуть використовуватися багатьма пристроями Інтернету речей з різних причин. Сучасні методи анонімізації і величезне число пристроїв Інтернету речей, підключених до мереж зв'язку загального користування (МЗЗК), роблять сучасні мережі і системи зв'язку уразливими перед зловмисниками. Уразливість мережевої безпеки, що полягає в неможливості аутентифікації пристроїв Інтернету речей, відкриває для зловмисників можливість для виробництва контрафактної фізичних і віртуальних речей.

Одним з напрямків забезпечення гарантованої і однозначної ідентифікації пристроїв Інтернету речей (IP) є використання унікального ідентифікатора пристрою IP в МЗЗК в сукупності з параметрами самого пристрою. При цьому треба враховувати, що так званий універсальний ідентифікатор повинен підтримувати (бути сумісний) з уже існуючими методами ідентифікації, такими як IMEI, MAC і інші.

Необхідно також відзначити, що від рівня до рівня ідентифікація пристроїв може підмінятися, тобто кінцевому пристрою IoT з певною фізичною адресою канального рівня спочатку призначається відповідну логічну адресу на мережевому рівні, який в подальшому може бути замінений на ідентифікатор на рівні платформи. При цьому дуже важливою властивістю є фіксованість співвідношення ідентифікатора з фактичним пристроєм Інтернету речей (фізичною адресою), а також універсальність в застосуванні ідентифікатора в різних галузях.

З урахуванням того, що, за останніми даними, кількість вже підключених пристроїв на планеті досягає 9 мільярдів, які розташовані по всьому світу необхідно також враховувати підтримку всіх типів мов і децентралізацію систем реєстрації цифрових об'єктів в інтернеті, щоб забезпечити децентралізовану систему управління цифровими об'єктами.

У зв'язку з цим однією з найважливіших проблем є вибір системи ідентифікації для всіх пристроїв IP, підключених до МЗЗК. В якості унікального глобального ідентифікатора пропонується безліч різних програмних і апаратних рішень. Одним з рішень, яке задовольняє пропонованим вимогам щодо ідентифікації пристроїв і додатків інтернету речей є DOA (Digital Object Architecture).

DOA і її базова система резолюції "Handle system" була спочатку створена як система резолюції ідентифікаторів, що володіє достатньою гнучкістю використання. Ідентифікатори містять актуальну інформацію про об'єкт - розміщення, умови використання, ключі шифрування і т.д. Дворівнева система резолюції і розподілена архітектура технології дозволяє швидко відображати зміни властивостей об'єктів і використовувати власну бізнес-модель для кожного адміністратора і сервера.

У зв'язку з тим, що DOA найбільш повно задовольняє перерахованим вище вимогам розробка моделей і методів для ідентифікації пристроїв і додатків IP на базі DOA є перспективним напрямком розвитку систем ідентифікації.

Літератури:

1. Recommendation ITU-T T.181203 : An architecture for IoT interoperability. – Geneva: ITU-T, 2018 – 25.

2. Владимиров, С.С. Методика идентификации устройств Интернета вещей на основе принудительной деградации участка флеш-памяти / С.С. Владимиров, Р.В. Киричек // Электросвязь. – 2017. – № 2. – С. 32–35.

3. Цифровая идентификация объектов: технология и не только; под ред. М.А. Медриша. – М.: Научное обозрение, 2016. – 228 с.

DEEPFAKE

Петросян Вадим Едуардович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Deepfake (дінфейк) - конкатенація слів «глибинне навчання» (англ. Deep learning) і «підробка» (англ. Fake), методика синтезу зображення, заснована на штучному інтелекті. Вона використовується для з'єднання і накладення існуючих зображень і відео на вихідні зображення або відеоролики. У переважній більшості випадків, для створення таких відео використовують генеративно-змагальні нейромережі (GAN). Одна частина алгоритму вчиться на реальних фотографіях певного об'єкта і створює зображення, буквально «змагаючись» з другою частиною алгоритму, поки та не почне плутати копію з оригіналом.

Останнім часом технологічні гіганти на кшталт Microsoft і Facebook займалися розробкою ПЗ, здатного з високою точністю визначати підроблені відео, засновані на нейромережі Deepfake. Як виявилося, подібні системи легко обдурити, що недавно довели програмісти з США.

Група вчених з Каліфорнійського університету в Сан-Дієго представила результати дослідження на конференції з комп'ютерного зору WACV 2021. За їх словами, досить використовувати так звані «змагальні» приклади, що представляють собою змінені вхідні дані в кожному окремому кадрі відеопотоку. З'ясувалося, що подібний метод працює навіть після стиснення і постобробки.

Нейронні мережі, які вміють виявляти підроблене відео, концентруються на елементах, які сучасні алгоритми Deepfake поки не здатні якісно обробляти. В першу чергу це миготіння і деякі інші сцени. Виявилося, що в даному випадку зловмисникові досить мати знання про особливості роботи ПО, що виявляє підроблене відео.

Так, якщо автори Deepfake мали повний доступ до моделі детектора, то ймовірність обману системи доходила до 99%. У той же час, якщо зловмисник мав лише частковий доступ до програмного забезпечення, то шанси створити відеоряд, що проходить перевірку, знижувалися до 86%. Автори методики відмовилися викладати її у відкритий доступ.

Важко зробити хороший фейк на звичайному комп'ютері. Більшість із них створені на висококласних робочих столах з потужними графічними картами або, ще краще, з обчислювальною потужністю у хмарі. Це скорочує час обробки з днів і тижнів до годин. Але потрібен досвід, не в останню чергу, щоб підправити завершені відеоролики, щоб зменшити мерехтіння та інші дефекти зору. Тим не менше, багато інструментів тепер доступні, щоб допомогти людям зробити deepfakes. Кілька компаній виготовлять їх для вас і виконують всю обробку в хмарі. Існує навіть додаток для мобільних телефонів, Zao, який дозволяє користувачам додавати свої обличчя до списку телевізійних та кінофільмів.

Чи завжди deepfake зловмисні? Зовсім ні. Багато розважають, а деякі корисні. Клонування голосу за допомогою DeepFake може відновити голос людей, втрачений через хворобу. DeepFakes можуть оживити галереї та музеї. У Флориді в музеї Далі є копія художника-сюрреаліста, який представляє своє мистецтво та робить селфі з відвідувачами. Для індустрії розваг технологія може бути використана для вдосконалення дубляжу на іноземномовних фільмах і, що є більш суперечливим, для воскрешення мертвих акторів. Наприклад, покійний Джеймс Дін повинен зіграти роль у фільмі "В пошуках Джека", фільмі про війну у В'єтнамі.

Література:

1. https://www.proglib.io/p/deepfake-tutorial-sozdaem-sobstvennyy-dipfeyk-v-deepfacelab-2019-11-16

2. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

РОЗВИТОК ПОНЯТТЯ BIG DATA ТА ОБГРУНТУВАННЯ ВАЖЛИВОСТІ ПРОЦЕСУ

Петрунчак Анна Романівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Не секрет, що на сьогодні об'єми даних, які вимагається зберігати і обробляти, ростуть в геометричній прогресії. Наприклад, об'єми даних, які зберігаються в Інтернет, збільшуються приблизно на 40 % щорічно. З одного боку, саме розвиток сучасних інформаційних технологій дозволяє і сприяє тому, щоб об'єми оброблюваних даних, що зберігаються і, постійно росли. А з іншого, для роботи зі швидкорослими об'ємами найрізноманітніших видів даних потрібно все більше ресурсів і складніших програмних рішень. Однією з найбільш сучасних і швидко набираючих популярність технологій є big data. Вже сьогодні найбільші світові компанії, що займають лідируючі позиції в самих різних областях бізнес діяльності, вкладають мільярди доларів в розвиток цього напряму.[1]

Визначення BigData

Під термінами "BigData", ховається величезний набір інформації, чиї масштаби, різноманітність і складність якого вимагає нових архітектури, методів, алгоритмів і засобів аналізів для управління нею. Взагалі цей напрям досить новий і далеко не усі розуміють сенс терміну BigData. Так само доки не існує точного визначення цього терміну. При цьому необхідність в нім збільшується з кожним роком. Головне завдання BigData - здатність обробляти великі об'єми не структурованих даних і видавати на їх основі певний прогноз. GoogleTrends показує початок активного зростання вживання словосполучення починаючи з 2011 року.

Особливості застосування і роль в сучасному бізнесі

Вивчаючи різноманіття сучасних технологій зберігання і обробки даних, виникає логічне питання. Для чого придумані методи і підходи, що називаються big data? Що в цьому унікального, як можна використати інформацію, оброблену за допомогою цих технологій і чому компанії готові вкладати в розвиток великих даних величезні кошти?

По-перше, на відміну від big data, звичайні бази даних (БД), не можуть зберігати і обробляти такі величезні об'єми даних (сотні і тисячі терабайт). І мова навіть не про аналітику, а тільки про зберігання даних. У класичному розумінні БД призначена для швидкої обробки (зберігання, зміна) відносно невеликих об'ємів даних або для роботи з великим потоком записів невеликого розміру, як транзакційна система. За допомогою big data якраз вирішується це основне завдання - успішне зберігання і обробка великих об'ємів даних.

По-друге, в big data структуруються різнотипні відомості, які поступають з різних джерел (зображення, фото, відео, аудіо і текстові документи) в один єдиний, зрозумілий і прийнятний для подальшої роботи вид.

По-третє, в big data відбувається формування аналітики і побудова точних прогнозів на підставі отриманої і обробленої інформації.

Один з найбільш наочних і популярних на сьогодні прикладів, про який можна прочитати у багатьох джерелах мережі Інтернет, пов'язаний з компанією Apple, яка збирає дані про своїх користувачів за допомогою вироблюваних пристроїв: телефон, планшет, годинник, комп'ютер. Саме із-за наявності такої системи корпорація володіє величезною кількістю інформації про своїх користувачів і надалі використовує її для отримання прибутку. І подібних прикладів на сьогодні можна знайти цілу множину.[2]

Короткий огляд інструментів BigData

Враховуючи величезні об'єми інформації, які необхідно зберігати обробляти в процесі роботи, слід зауважити, що подібні маніпуляції не можуть виконуватися на простих жорстких дисках. А програмне забезпечення, яке структурує і аналізує накопичувані дані, - це окрема інтелектуальна власність і у кожному окремому випадку є авторською розробкою. При цьому можна відмітити найбільш популярні на сьогодні інструменти, на основі яких створюються такі рішення:

– Hadoop & MapReduce;

– NoSQL бази даних;

– Інструменти класу Data Discovery.[3]

Висновок

У сучасному бізнесі, практично не залежно від специфіки та індустрії, усе більше простежується цінність і висока роль інформації про потенційних і поточних клієнтів компанії, про її конкурентів і прийдешні тенденції на ринку. У зв'язку з цим і вже існуючими прикладами успіху впровадження big data великими компаніями, якими наповнений Інтернет, можна припустити, що роль великих даних з часом тільки ростиме.

Література:

1. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим/ В. М. Шенбергер, К. Кукьер; пер. с англ. Инны Гайдюк. – М.: Манн, Иванов и Фербер, 2018. – 240 с

2. Коновалов, М. В. Big Data. Особливості і роль в сучасному / Технічні науки: проблеми і перспективи. - Санкт-Петербург : Своє видавництво, 2018. - С. 8-10.

3. MapReduce and Teradata Aster SQL - MapReduce // Teradata. URL: https://www.teradata.com/products-and-services/Teradata-Aster/teradata-aster-sql-mapreduce

ІТ-ТЕХНОЛОГІЇ В СПОРТІ

Подзігун Андрій Андрійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних тенологій

м. Київ

Спорт вважається видатним сектором промисловості у всьому світі, і його можна визначити в різних сферах з точки зору бізнесу: наприклад, змагальний спорт, відпочинок, фітнес та розваги. Усі ці сфери були повторно помітно перетворені цифровими технологіями. За останні три десятиліття дисципліна спортивна інформатика стала зростаючою дисципліною. У сучасному зв'язаному світі використання технологій, що носяться, аналізу великих даних, соціальних медіа та сенсорних технологій зробило революцію в тому, як спорт грається, аналізується та вдосконалюється.

Завдяки різним сучасним досягненням та програмам, професійні спортсмени можуть отримати глибше розуміння своєї діяльності, вдосконалити методи тренувань та підвищити

свої навички. На додаток до цього, шанувальники шукають мобільні додатки, щоб дати їм найсвіжішу статистику про улюблених гравців; в режимі реального часу, за кадром вміст у поєднанні з миттєвою реакцією, як спортсменів, так і побратимів Вони хочуть максимумів, мінімумів, реміксів, шукають зв'язок поза грою і хочуть поділитися досвідом з однодумцями вболівальників.

Події є головним моментом у спорті. Спортивний клуб повинен управляти кількома іграми, оптимізуючи цінність, яку він може створити для вболівальників, і максимізуючи прибуток, який вони можуть отримати від них. Для спортивних фірм оцифровані товари спортивного споживання - це чудова можливість надавати свій вміст та послуги в індивідуальному порядку.

Присутність соціальних медіа мала величезний вплив на кожен аспект нашого життя за останні десять років, і спорт також не є винятком. Соціальні мережі сильно змінили взаємодію між сортувальниками, клубами та прихильниками. Сьогодні тісний зв'язок між спортивними подіями та соціальними мережами є безперечним. Більшість команд, чемпіонатів чи спортивних асоціацій мають принаймні один медіа-профіль (Twitter, Facebook, Instagram, Youtube тощо).

Діджиталізація розширює екосистему спортивних організацій як нових зацікавлених сторін в галузі IT, таких як постачальники програмного забезпечення та постачальники даних. Наприклад, успіх німецької національної збірної з футболу у використанні аналітичних даних на турнірі Кубка світу значною мірою був підтриманий постачальником програмного забезпечення. Система розвідки талантів також зазнала революції. Наявність величезної кількості статистичних даних, створених різними носіями датчиків та аналітичними інструментами, призводить до того, що розвідка та вербування гравців ще більше залежать від даних, а не від інтуїції та від очей.

Діджиталізація може допомогти клубу в різних сферах:

- управління інфраструктурою та безпекою;
- пошук талантів;
- управління командою;
- спонсорство та управління постачальниками.

Інформатика в спорті - це безкрає поле досліджень та розробок. Унікальне поєднання спортивної науки та інформатики з великою сферою застосування спорту на будь-якому рівні дає великі перспективи. Величезний обсяг даних, що генеруються різними цифровими засобами (пристроями,

датчиками, аналітичними інструментами, камерами тощо), стає все більш доступним, простежуваним і видимим для всіх членів спортивних організацій, а також для любителів спорту. Важливість використання аналітичних даних є надзвичайно важливою для підвищення ефективності діяльності спортсменів, команд та клубів. Отже, використання інформаційних технологій створює конкурентні переваги для спортивних організацій.

Найважливішою групою у світі професійного спорту є її споживач. Діджиталізація зробила революцію у споживанні спорту та мотиваційній поведінці прихильників. Сьогодні ще більше вболівальників люблять отримувати гіперінформацію про щоденні новини, бути завжди на зв'язку з улюбленою командою, слухати враження та інтерв'ю спортсменів та тренерів, бачити, як виступають гравці, іншими словами: залишатися на зв'язку. Шанувальники отримали доступ до відповідного контенту, отримали можливість поділитися своїм досвідом на різних сайтах соціальних медіа під час заходу та отримати більш індивідуальний досвід.

Література:
1.https://www.intellectsoft.net/blog/
2.https://www.globalsportsjobs.com/article/
3.https://www.linkedin.com

ГОЛОГРАФІЧНИЙ ДИСПЛЕЙ З ДОПОВНЕНОЮ РЕАЛЬНІСТЮ AR HUD

Поліщук Єлизавета Андріївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В століття високих технологій науково-технічний прогрес не стоїть на місці. Наука постійно шукає способи зробити працю людини простішою, цікавішою та більш автоматизованою. Автомобілісти – не виняток. Так, для автомобілів нового покоління компанія Panasonic Automotive представила на міжнародній виставці CES-2021 голографічний Head-Up дисплей зі штучним інтелектом та технологією доповненої реальності – AR HUD.

Використовуючи останні розробки в області обробки зображень, оптики, проекцій, а також штучного інтелекту, підтримувані контролером домену салону SPYDR, інженери Panasonic сконструювали інноваційну систему візуальної допомоги водієві.

Новий AR HUD об'єднує фізичну і доповнену реальність, проектуючи на лобове скло яскраву двоплощинну лазерну голографію високого дозволу, що відображає значущу для водія

інформацію - дані про дорожню ситуацію в режимі real-time, що оновлюються кожні 300 мілісекунд, multiply-навігацію, швидкість руху, залишок палива, кілометраж і т.п.

Крім того, система точно відстежує напрям погляду водія, а також переміщення об'єктів навколо автомобіля, що рухається, і відповідно до цього динамічно підлаштовує (зміщує) голограми і зображення доповненої реальності, уникаючи «розсинхрону». Тобто система проектує інформацію на рівні очей водія в залежності від того, в який бік він дивиться.

За словами президента Panasonic Automotive і виконавчого директора Panasonic Smart Mobility, Скотта Кірчнера, HUD - одна з найбільш швидко зростаючих категорій ринку транспортних засобів, однак традиційні індикатори на лобовому склі покривають лише невелику ділянку дороги. Рішення Panasonic охоплюють більше дорожнього простору і при цьому поєднують стандартну інформацію (дані про швидкість руху і запасі палива) з 3D-проекціями на об'єкти в далекому полі, навігаційної та іншою важливою інформацією, яка накладається на дорожнє простір попереду. Враховуючи, що кількість безпілотних транспортних засобів буде рости, цей AR HUD зможе забезпечити впевненість і підвищений комфорт для пасажирів, що дуже важливо.

За попередніми даними, масове використання подібних розробок може початись вже з 2023 року.

Література:

1. *https://zhuk.ua/ru/statti-ta-ohliady/golografichniy-displey-panasonic-head-up/*
2. *https://panasonic.ru/press_center/news/detail/474697*

РОЗУМНА ЗАХИСНА МАСКА PROJECT HAZEL

Поліщук Єлизавета Андріївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В реаліях 2021-го року неможливо уявити велике скупчення людей в громадському місці без масок. Майже цілий рік вона є нашим невід'ємним атрибутом і навіть символом повсякдення. Не дивно, що на нещодавній виставці CES-2021 була представлена найрозумніша захисна маска в світі – Project Hazel.

Виробник геймерських аксесуарів Razer вирішив долучитися до боротьби з коронавірусом і продемонстрував на CES-2021 багаторазовий респіратор Project Hazel, «найрозумнішу маску для обличчя в світі». Вона є стійкою до подряпин та водонепроникною. При цьому маска обладнана змінними модулями з високою ефективністю фільтрації

бактерій. Матеріали, з яких виготовлена маска – силікон та пластик, що переробляється.

За словами представників Razer, завдяки своєму прозорому дизайну, Project Hazel дозволяє іншим бачити вашу міміку (на відміну від звичайної маски), що покращує соціальну взаємодію. Дизайн Project Hazel спрямований на вирішення цієї проблеми. Як і слід було очікувати, маска Project Hazel не позбавлена ключової особливості сучасних продуктів фірми Razer. Вона оснащена RGB-підсвічуванням. Тому, якщо ви носите цю маску в темряві, підсвічування включається автоматично.

Для фільтрації повітря на вдих і видих в Project Hazel використовуються два клапани з активною вентиляцією, що не дозволяють масці пітніти. Razer стверджує, що її респіратор відповідає американському стандарту N95, тобто відфільтровує не менше, ніж 95% бактерій.

Project Hazel використовує також технологію VoiceAmp, яка використовує вбудований мікрофон і підсилювач для поліпшення голосу користувача. Однак виробник заявляє, що динаміки, якими обладнаний мікрофон, забезпечують невелике підсилення. І режиму «мегафону» тут немає. Розумна маска оснащена герметичним ущільненням регульованих вушних петель, активним повітряним охолодженням і пристроєм для швидкої бездротової зарядки, який за допомогою ультрафіолетового світла може дезінфікувати маску.

Коли саме маска буде доступною для широкого використання – поки невідомо. Планується, що в продажу вона буде йти в комплекті з кейсом для зарядки та одночасної дезінфекції.

Література:

1. https://www.ixbt.com/news/2021/01/13/predstavlena-samaja-umnaja-zashitnaja-maska-v-mire.html

2. https://www.hardwareluxx.ru/index.php/news/consumer-electronics/gadgets/50950-project-hazel-razer-rgb.html

3. https://mind.ua/ru/publications/20220850-ces-2021-10-vau-novinok-glavnoj-vystavki-elektroniki

ПРИНЦИП ПОШУК КЛЮЧОВИХ СЛІВ І ФРАЗ ПРИ ОБРОБЦІ ВЕЛИКИХ ОБЄМІВ ДАНИХ

Прокопів Назар Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Тематичний збір даних заснований на використанні опису теми, яке може складатися з ключових слів або фраз. Опис теми може складатися з десятків і сотень ключових слів і фраз, тому виникає задача їх швидкого пошуку в текстах. Пошук ключових слів і фраз відбувається в режимі реального часу і

здійснюється для всіх нових текстів, які були завантажені на останній ітерації роботи системи.

Процес пошуку ключових слів у документі ускладнює наявність «патернів» слів, які прагнуть врахувати різні словоформи слів. Відмітимо, що під фразами може розумітися як набір слів, що зустрічаються послідовно один за іншому в тексті, так і послідовність слів, які знаходяться на деякій відстані один від одного, а так само слова невпорядковані один щодо одного.

Дане узагальнене поняття фрази так само ускладнює процес їх пошуку в тексті.

Необхідність здійснювати пошук ключових слів у режимі реального часу не дозволяє здійснити «індексацію» документів - процедуру, при якій буде можливо організувати швидкий пошук по слову списку всіх документів, які його містять.

Одним з підходів, який міг би бути використаний для вирішення означеної завдання, є використання регулярних виразів. На підставі списку ключових слів може бути автоматично складено велику регулярний вираз, яке здійснює пошук цих слів в тексті. При цьому можуть бути автоматично враховані різні словоформи ключових слів. Однак на практиці цей підхід виявився не ефективним, оскільки час роботи алгоритму збільшується нелінійно взалежності від числа ключових слів. На темах описуваних десятками ключових слів, час роботи даного алгоритму значно збільшувалася.

Тому для пошуку ключових слів був використаний підхід, заснований на побудові префіксного дерева, що реалізує пошук безлічі підрядок зі словника в цьому рядку. На підставі ключових слів, що описують тему, будується префіксне дерево і реалізується алгоритм Ахо-Корасіка для пошуку підрядків подається на вхід рядку. Алгоритм дозволяє знайти всі входження в текст всіх ключових слів, що описують тему. Оскільки ключові слова мають безліч словоформ, то префіксне дерево будується виходячи з кореневих форм слів. потім на підставі інформації про становище в тексті цієї кореневої форми, перевіряється, що в тексті дійсно міститься вказане в словнику ключове слово. Таким чином даний алгоритм дозволяє здійснювати швидкий пошук ключових слів у безлічі текстів.

Пошук фраз здійснюється на основі знайдених в тексті ключових слів. В загальному випадку під фразою розуміється модель «мішка слів» (bag of words) [2], при якій не фіксується ні послідовність слів, ні відстань між ними, хоча ці обмеження так само можуть бути враховані. Наприклад, в рамках моделі мішка слів, наявність в тексті фрази «купити машину» означає, що в

тексті містяться два ключових слова: «Купити» і «машина». Відзначимо, що порядок розташування слів і відстані між ними так само можуть бути враховані описуваних алгоритмом пошуку фраз.

В рамках моделі мішка слів, кожна фраза описується неврегульованим безліччю ключових слів. Тексти так само описуються неупорядкованими множинами слів. Для перевірки наявності ключової фрази в тексті необхідно перевірити, що безліч всіх ключових слів фрази міститься у великій кількості слів тексту. Оскільки опис теми може складатися з великої кількості фраз, дану процедуру необхідно проводити велику кількість разів.

Для швидкого пошуку всіх ключових фраз в тексті використовуються наступний алгоритм. Всі ключові слова ранжуються виходячи з частоти їх появи в ключових фразах. Слово, що зустрічається в безлічі ключових фраз найчастіше, має мінімальним рангом. Для опису фрази - що входять до неї слова упорядковано виходячи з значення свого рангу. Слова упорядковано для того, щоб можна було виробляти пошук підмножини в безлічі за лінійний час. Потім для кожної фрази вибирається слово представник - слово, яке міститься у фразі і має максимальний рангом. На основі цих даних створюється асоціативний масив, який за словом дозволяє отримати список всіх фраз, які воно є словом представником [3].

У тексті проводиться пошук всіх ключових слів, які так само упорядковано виходячи зі свого рангу. Потім ці слова аналізуються в порядку зменшення рангу. Для кожного слова, використовуючи побудований на початку роботи асоціативний масив, виходить список фраз, для яких воно є представником. Для цього невеликого списку фраз перевіряється їх входження в текст. Оскільки списки ключових слів в тексті і у фразі сортовані в однаковому порядку, то перевірка на входження одного безлічі в інше може бути ефективно здійснена за лінійний час від їх розмірів.

Даний підхід виявився ефективним і в разі роботи з тисячами фраз. Після визначення фрази в тексті можуть бути враховані обмеження на порядок слів і відстань між ними. Для цих цілей для кожного знайденого в тексті ключового слова фіксується його позиція в тексті: кількість символів з початку тексту і номер цього слова в тексті. На підставі цих даних можуть бути визначені відносні позиції слів один щодо одного, а так само число слів між ними.

Література:

1. Shakhovska N. Data space architecture for Big Data managering/ N. Shakhovska, O. Veres, Y. Bolubash, L. Bychkovska-Lipinska/ Xth International Scientific and Technical Conference "Computer Sciences and Information Technologies" (CSIT'2015).- P. 184-187, Lviv, 2015.

2. Шаховська Н. Б. Організація великих даних у розподіленому середовищі / Н. Б. Шаховська, Ю. Я. Болюбаш, О. М. Верес // Обчислювальна техніка та автоматизація:- Донецьк, 2017. - С. 147-155.

3. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим/ В. М. Шенбергер, К. Кукьер; пер. с англ. Инны Гайдюк. – М.: Манн, Иванов и Фербер, 2018. – 240 с

СУЧАСНИЙ ПІДХІД КЕРУВАННЯ КЛАСТЕРУ КОНТЕЙНЕРІВ LINUX ЗА ДОПОПОМОГОЮ KUBERNETES

Путін Олександр Геннадійович
Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій
м. Київ

Постановка задачі. Ознайомити слухачів з системою керування застосунками у контейнерах Kubernetes.

Мета дослідження. Поділити інформацію на наступні теми:

– Що таке Kubernetes

– Чому потрібен Kebernetes та його функціонал

– Чим не являється Kubernetes

Результати дослідження. Kubernetes (або ж скорочено K8s) — відкрита система автоматичного розгортання, масштабування та управління застосунками у контейнерах. Розроблена компанією «Google». Система підтримує ряд інструментаріїв з управління контейнерами, у тому числі Docker [1].

Kubernetes визначає набір будівельних блоків («примітивів»), які спільно забезпечують механізми для розгортання, підтримки та масштабування застосунків. Kubernetes слабко зв'язний, та розширюваний, щоб відповідати різноманітним робочим навантаженням. Розширюваність в основному забезпечується за допомогою Kubernetes API, що використовується внутрішніми компонентами, а також розширеннями та контейнерами, що працюють на Kubernetes [2].

Kubernetes має наступний функціонал:

– Виявлення сервісів та балансування навантаження. Kubernetes може надавати доступ до контейнера, використовуючи DNS-ім'я або його власну IP-адресу. Якщо контейнер зазнає завеликого мережевого навантаження, Kubernetes здатний збалансувати та розподілити його таким чином, щоб якість обслуговування залишалась стабільною.

– Оркестрація сховища інформації. Kubernetes дозволяє автоматично монтувати системи збереження інформації на вибір: локальні сховища, рішення від хмарних провайдерів тощо.

– Автоматичне розгортання та відкатування. За допомогою Kubernetes можна описати бажаний стан контейнерів, що розгортаються, і він простежить за виконанням цього стану. Наприклад, можна автоматизувати в Kubernetes процеси створення нових контейнерів для розгортання, видалення існуючих контейнерів і передачу їхніх ресурсів на новостворені контейнери.

– Автоматичне розміщення задач. Kubernetes розподіляє контейнери по вузлах кластера для максимально ефективного використання ресурсів ЦПУ та пам'яті (RAM) [3].

– Самозцілення. Kubernetes перезапускає контейнери, що аварійно завершились; заміняє контейнери; зупиняє роботу контейнерів, що не відповідають на задану користувачем перевірку стану, і не повідомляє про них клієнтам, допоки ці контейнери не будуть у стані робочої готовності.

– Управління секретами та конфігурацією. Kubernetes дозволяє зберігати та керувати чутливою інформацією, такою як паролі, OAuth токени та SSH ключі.

– Kubernetes намагається підтримувати найрізноманітніші типи навантажень, включно із застосунками зі станом (stateful) та без стану (stateless), навантаження по обробці даних тощо. Якщо застосунок можна контейнеризувати, він чудово запуститься під Kubernetes.

Kubernetes не є комплексною системою PaaS (Платформа як послуга) у традиційному розумінні. Оскільки Kubernetes оперує швидше на рівні контейнерів, аніж на рівні апаратного забезпечення, деяка загальнозастосована функціональність і справді є спільною з PaaS, як-от розгортання, масштабування, розподіл навантаження, логування і моніторинг. Водночас Kubernetes не є монолітним, а вищезазначені особливості підключаються і є опціональними. Kubernetes надає будівельні блоки для створення платформ для розробників, але залишає за користувачем право вибору у важливих питаннях.

Kubernetes - не просто система оркестрації. Власне кажучи, вона усуває потребу оркестрації як такої. Технічне визначення оркестрації - це запуск визначених процесів: спочатку A, за ним B, потім C. На противагу, Kubernetes складається з певної множини незалежних, складних процесів контролерів, що безперервно опрацьовують стан у напрямку, що заданий бажаною конфігурацією. Неважливо, як ви дістанетесь

з пункту А до пункту С. Централізоване управління також не є вимогою. Все це виливається в систему, яку легко використовувати, яка є потужною, надійною, стійкою та здатною до легкого розширення.

Література:

1. *"Kubernetes" [Електронний ресурс] - https://en.wikipedia.org/wiki/Kubernetes*
2. *"What is Kubernetes?" [Електронний ресурс] - https://kubernetes.io/docs/concepts/overview/what-is-kubernetes/*
3. *"Autoscaling based on CPU/Memory in Kubernetes" [Електронний ресурс] - https://blog.powerupcloud.com/autoscaling-based-on-cpu-memory-in-kubernetes-part-ii-fe2e495bddd4*

КОНТЕЙНЕРИЗАЦІЯ LINUX ЗАСТОСУНКІВ ЗА ДОПОМОГОЮ DOCKER

Путін Олександр Геннадійович
Навчально-науковий інститут інформаційних технологій
Державний університет телекомунікацій
м. Київ

Постановка задачі. Ознайомити слухачів з інструментарієм для управління ізольованими Linux-контейнерами Docker.

Мета дослідження. Поділити інформацію на наступні теми:

- Визначення технології
- Переваги Docker
- Приклади використання

Результати дослідження. Docker - програмне забезпечення для автоматизації розгортання і управління додатками в середовищах з підтримкою контейнеризації. Дозволяє «упакувати» додаток з усім його оточенням і залежностями в контейнер, який може бути перенесений на будь-яку Linux-систему з підтримкою cgroups в ядрі, а також надає середовище з управління контейнерами. [1]

Переваги використання Docker:

1. **Мінімальне споживання ресурсів** - контейнери не віртуалізують всю операційну систему (ОС), а використовують ядро хоста і ізолюють програму на рівні процесу. Останній споживає набагато менше ресурсів локального комп'ютера, ніж віртуальна машина.
2. **Швидкісне розгортання** - допоміжні компоненти можна не встановлювати, а використовувати вже готові docker-образи (шаблони). Наприклад, не має сенсу постійно встановлювати і налаштовувати Linux Ubuntu. Досить 1 раз її

інсталювати, створити образ і постійно використовувати, лише оновлюючи версію при необхідності.

3. **Зручне приховування процесів** - для кожного контейнера можна використовувати різні методи обробки даних, приховуючи фонові процеси.

4. **Робота з небезпечним кодом** - технологія ізоляції контейнерів дозволяє запускати будь-який код без шкоди для ОС.

5. **Просте масштабування** - будь-який проект можна розширити, запровадивши нові контейнери.

6. **Зручний запуск** - додаток, що знаходиться всередині контейнера, можна запустити на будь-якому docker-хості.

7. **Оптимізація файлової системи** - образ складається з шарів, які дозволяють дуже ефективно використовувати файлову систему. [2]

Основні приклади використання:

1. **Швидка доставка додатків** (команди docker pull і docker push) дозволяє організувати колективну роботу над проектом. Розробники можуть працювати віддалено на локальних комп'ютерах і виконувати пересилання фрагментів коду в контейнер для тестів.

2. **Розгортання і масштабування** - контейнери працездатні на локальних комп'ютерах, серверах, в хмарних онлайн-сервісах. Їх можна завантажувати на хостинг для подальшого тестування, створювати (docker run), зупиняти (docker stop), запускати (docker start), припиняти і відновлювати (docker pause і docker unpause відповідно).

3. **Множинні навантаження** - здійснення запуску великої кількості контейнерів на одному і тому ж обладнанні, оскільки Docker займає невеликий обсяг дискової пам'яті.

4. **Диспетчер процесів** - можливість моніторингу процесів в Docker за допомогою команд docker ps і docker top, що мають схожий синтаксис з Linux.

5. **Зручний пошук** - в реєстрах Docker він здійснюється дуже просто. Для цього слід використовувати команду docker search. [3]

Docker є важливим інструментом для кожного сучасного розробника, як основа апаратної віртуалізації додатків. Ця технологія має широкий функціонал і можливостями для контролю процесів. Докер дозволяє не тільки розгортати контейнери, а й оперативно масштабувати їх екземпляри, працювати з многоконтейнернимі додатками (Docker Compose), а також об'єднувати кілька Докер-хостів в єдиний кластер (Docker Swarm).

Докер характеризується досить простим синтаксисом. Тому він досить простий в освоєнні як для досвідчених IT-фахівців, так і для новачків. Програмне забезпечення сумісне з усіма версіями операційних систем Linux і Windows, тому область застосування Docker практично не обмежена.

Література:

1. “ Docker (software)” [Електронний ресурс] - https://en.wikipedia.org/wiki/Docker_(software)

2. “ Що таке Docker і як його використовувати в розробці?” [Електронний ресурс] - https://eternalhost.net/blog/razrabotka/chto-takoe-docker

3. “What can I use Docker for?” [Електронний ресурс] - https://docs.docker.com/get-started/overview/#what-can-i-use-docker-for

ЯК БУДУТЬ ЗБЕРІГАТИСЯ ДАНІ У МАЙБУТНЬОМУ

Руденко Віталій Дмитрович, Матвійчук Артем Миколайович, Луппа Олексій Андрійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

«Дані правлять світом. Як очікується, зростання сумарної кількості створюваних даних буде експоненціально прискорюватися і до 2025 року їх обсяг досягне 175 зеттабайт. Сьогодні ми створюємо більше даних за годину, ніж 20 років тому створювали за цілий рік. І, коли обсяги вимірюються зеттабайтами, нам потрібен простий, безпечний і недорогий спосіб збору, зберігання і застосування цих даних », - говорить Дейв Мослі (Dave Mosley), генеральний директор Seagate Technology.

На цей момент кількість цифрових даних у світі вимірюється міліардами терабайт. Перехід багатьох сфер в онлайн на фоні пандемії ще більше збільшив потік даних, що призвело до ускладнення і збільшення різноманіття екосистеми даних. Застосування Iot, AI, смарт-технологій призводить до збільшення попиту на обчислювальні ресурси [1].

По-пенше, у майбутньому будуть широко використовуватися об’єктні сховища, які зараз використовуються у хмарних сховищах. Головними перевагами об’єктних сховищ є: масштабованість (об’єктні сховища можуть містити майже будь-яку кількість даних без необхідності розбиття даних на розділи), ефективність (відсутність ієрархії означає відсутність проблем, пов’язаних з використанням складних систем каталогів), доступність (об’єктні системи зберігання мають механізми для збереження цілісності даних, забезпечують реплікацію даних та послідовні оновлення даних).

По-друге, у інформаційних сховищах майбутнього буде використовуватись архітектура збереження даних, розділена на рівні. Дані, які часто використовуються, зберігатимуться на флеш-накопичувачах, а все інше - на дискових пристроях.

Наприклад, конструкція графічних процесорів NVIDIA передбачає поділ пам'яті на рівні - регістри, спільна пам'ять і глобальна пам'ять. У кожного рівня свої характеристики. У регістрів мінімальна затримка доступу, але обсяг пам'яті цього типу невеликий. А обсяг глобальної пам'яті великий, але і затримка більша. В NVIDIA передбачили програмний інтерфейс для використання переваг багаторівневої пам'яті і програмування систем, оптимізованих для такої архітектури. За аналогією твердотільні накопичувачі і жорсткі диски можна застосовувати на різних рівнях сховища [2]. Сьогодні, коли генеруються дуже великі обсяги корисних даних, використовувати для них однорідне сховище було б неефективно. Тож така схема ієрархії забезпечує найбільш ефективний баланс між ціною та продуктивністю.

По-третє, використання формативного AI у сфері зберігання даних призведе до збільшення корисності даних. На фоні росту кількості даних збільшується і кількість корисної інформації, тож потрібен інструмент, який би зміг швидко обробити великі обсяги даних та зберегти найголовніше. Формативний AI допоможе у цьому, адже він може адаптуватися до сфери, у якій працює, а також генерувати нові алгоритми для рішення конкретних задач [3], що є дуже важлимим при роботі з великими обсягами даних.

Отже, кількість сворених даних у майбутньому буде тільки зростати, тож ми потребуємо технології, які допоможуть у зберіганні, обробці та швидкому доступу до них. У даній тезі представлено декілька технологій, які будуть широко використовуватись у майбутньому у сфері даних.

Література:

1. *https://www.itworld.ru/tech/technology/168855.htmlhttps://www.who.int/en/news-room/fact-sheets/detail/electromagnetic-fields-and-public-health-mobile-phones*
2. *https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/*
3. *https://www.ibm.com/ru-ru/cloud/learn/what-is-object-storage*

ПРИНЦИПИ САМОВДОСКОНАЛЕННЯ В IT СФЕРІ

Рудська Анастасія Ігорівна
Державний Університет Телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Проектна робота розроблена на основі React Native за допомогою Expo та Visual Studio. React Native - це фреймворк мобільних додатків з відкритим кодом [1]. Пропонує користувачам вдосконалювати свої навички та розвиватися в IT сфері.

Постійне самовдосконалення та висока активність - запорука успіху. ІТ-ринок швидко зростає, тож фахівці мають миттєво реагувати на зміни та відповідати актуальним потребам ринку праці [2].

Якщо у вас недостатньо досвіду, акцентуйте увагу на навичках, якими вже володієте, над чим працюєте та що плануєте опанувати. Проходження курсів, вебінарів, відвідування конференцій неодмінно допомагає розвиватися та вдосконалювати свої навички. Найвідоміші онлайн курси світу: Coursera, Udemy, Edx, CodeAcademy, Prometheus, rubymonk [3].

Мій додаток містить в собі курси, які зібрані з різних навчальних сайтів. За допомогою пошуку, користувач може знайти курс за темою, яка йому необхідна, відсортувати за рейтингом та за вартістю, обрати необхідний та перейти за посиланням вже на обраний сайт, щоб придбати курс.

Цей додаток розроблений для користувачів, які бажають та прагнуть до самовдосконалення, саморозвитку. Додаток допомагає людям знайти навчальний курс за темою яка їх цікавить або необхідна. Таким чином, людині не треба ходити по всіх сайтах з курсами, та шукати той самий для себе, все є в одному додатку. Шукаєш, сортуєш, обираєш, навчаєшся.

Література:

1. *Inspired.com Url:https://inspired.com.ua/ideas/services/10-sites-coding-online/*
2. *Official documentation ReactNative Url: https://reactnative.dev/docs/getting-started*
3. *RozvitokIT Article-November, 2018 Url: https://rozvitokit.com/do/article2018/*

НОУТБУК З ДВОМА ЕКРАНАМИ

Савицький Костянтин Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В світі ноутбуків давно не відбувалось революцій. Верхньою частиною, що відкривається на 360°, перетворюючи ноутбук на планшет, нікого не здивуєш. Як і корпусом з алюмінію. Але в цей час компанія ASUS кілька років вивчала способи монтування додаткових дисплеїв до ноутбуків. Демонстрація даного продукту на виставці CES-2021 довела, що в цій розробці є сенс.

Першим експериментом фірми ASUS був маленький додатковий екран ScreenPad, що розташовувався під тачпадом. Нинішній додатковий сенсорний екран ScreenPad Plus за шириною не поступається основному. Його можна піднімати на 9.5 градусів і використовувати для розміщення додаткових налаштувань різних додатків (наприклад, Photoshop).

Два виставлених на CES ноутбука ZenBook Duo з діагоналями 14 і 15,6 дюймів продемонстрували, наскільки ASUS просунув свої технології. Його нові екрани стали зручніше і краще відображають кольору. Також компанія удосконалила програмне забезпечення, спростивши розподіл завдань між двома дисплеями.

На перший погляд додатковий екран ScreenPad + здається непотрібним. Справді, є ж основний, 15-дюймовий, з роздільною здатністю 4K, 3840x2160 пікселів. Але виробник непогано допилив ПЗ ноутбука, так що другий екран є буквально продовженням основного, маючи такий же дозвіл 4K, 3840x1100 пікселів.

Рис. 1 – Ноутбук Asus ZenBook Duo 15,6'

Цей екран матовий, по ньому приємно водити пальцем, адже ScreenPad + сенсорний. При бажанні можна мишкою перетягнути відкриті вікна і додатки з основного на додатковий екран, і управляти ними дотиками.

Якщо використовувати ноутбук в якості друкарської машинки, то придумати ефективний сценарій використання відразу двох екранів буде проблематично. Але якщо писати музику, малювати чи займатися програмуванням - другий екран буде доречним.

Серед інших переваг цього ноутбука, які не відразу кидаються в очі - матриця екрану не IPS, а OLED. Для користувача це в першу чергу шикарний чорний колір, тому що підсвічування як таке відсутнє. У OLED-екранах кожен піксель сам є джерелом світла, тому на ділянках, де потрібно

відобразити чорний, пікселі просто не світяться. Плюс у ASUS ZenBook Pro Duo колірний обхват дорівнює 100% DCI-P3. Цей стандарт максимально наближений до кінематографічного, який давно підтримується ноутбуками Apple.

Також варто відзначити, що ефективність системи охолодження на високому рівні. У ноутбуці встановлений 6-ядерний Intel Core i7-9750H (доступний також топовий Core i9-9980HK) який «із задоволенням» розігрівається до граничних показників температури - 90-95 ° С. Але системі вдається утримуватися в цьому діапазоні. Так, кулери працюють на максимальних обертах, але їм вдається стримувати нагрів, не даючи процесору тротлити, знижуючи частоту. Показники синтетичних тестів показують, що Zenbook Pro Duo це не тільки продуктивний ноутбук для професійних завдань і вимогливих ігор, але і продуманий пристрій з набором цікавих ергономічних особливостей.

Література:

1. *https://mind.ua/ru/publications/20220850-ces-2021-10-vau-novinok-glavnoj-vystavki-elektroniki*
2. *https://hi-tech.ua/article/asus-zenbook-duo-and-zenbook-pro-duo-test/*
3. *https://www.iphones.ru/iNotes/noutbuk-s-dvumya-ekranami-asus-zenbook-duo-chto-za-zver-takoy-11-19-2019*

АНАЛІЗ ПЕРЕВАГ СТАНДАРТУ LORAWAN

Свідерський В.О.
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

В останні роки утворився новий напрямок розвитку технологій, що отримав назву Інтернету речей або IoT (Internet of Things). IoT є сукупністю розвитку мереж міжмашинних комунікацій і систем зберігання/обробки великих даних, коли за рахунок підключення датчиків і механізмів до мережі реалізується цифровізація різних процесів і об'єктів. Використання отриманих даних дозволяє проводити оптимізацію процесів і об'єктів на базі нових алгоритмів. Одна з перспективних технологій IoT є технологія LoRaWAN, яка сприяє вирішенню важливих технічних питань, та забезпечує масове розгортання IoT.

Серед незаперечних переваг у порівнянні з іншими стандартами - LoRaWAN:

- найбільш динамічно розвивається загальносвітова екосистема (понад 500 учасників TheLoRaAlliance. А це означає, що в усьому світі значно більше виробників датчиків, програмних рішень і мережевого устаткування в порівнянні з іншими стандартами.

- дуже низьке споживання енергії (наприклад, датчик для контролю житлово-комунального господарства може без заміни батареї пропрацювати до 10 років. Пристрої в мережі LoRaWAN асинхронно обмінюються даними тільки тоді, коли їм є, що передати. Можна задати передачу даних за розкладом або поза залежністю від конкретного часу.

У звичайних мобільних мережах пристрої часто змушені «прокидатися» для синхронізації з мережею і перевірки повідомлень для отримання і / або відправки. Така синхронізація призводить до значної витрати енергії і скорочує автономний термін роботи пристрою від акумулятора. Аналітики GSMA провели безліч досліджень мереж LPWAN, в результаті чого прийшли до висновку: автономність LoRaWAN-пристроїв в 3-5 разів вище в порівнянні з іншими технологіями.

- велика територія покриття однієї базової радіостанції (до 12 км - в умовах міста і понад 25 км - в сільській місцевості)

- ємність мережі.

Для забезпечення нормальної роботи мережі LPWAN шлюз повинен мати дуже високу пропускну здатність або можливість отримувати повідомлення з дуже великою кількістю кінцевих пристроїв. Висока ємність мережі LoRaWAN досягається за рахунок використання адаптивної швидкості передачі даних і використання багатоканального приймача в шлюзі, що гарантує одночасне отримання повідомлень на кількох каналах.

Шлюзи дозволяють одночасно по одному каналу отримувати інформацію з пристроїв, які використовують різні швидкості для передачі даних. Адаптивна швидкість для передавання даних також оптимізує час роботи акумулятора обладнання.

Мережі LoRaWAN можуть бути розгорнуті з мінімальною кількістю інфраструктури. У міру необхідності, в залежності від кількості пристроїв в мережі, можна змінювати швидкості передачі даних або збільшити кількість шлюзів.

На мережі IoT Ukraine вже реалізовані всі ключові рішення широкої палітри Інтернету речей і працюють сотні підключених пристроїв. Тепер всі великі міста, промислові підприємства і агрофірми отримали можливість, динамічно розвивати свої розумні екосистеми, скорочувати витрати і підвищувати ефективність. Перша Національна мережа для розумних девайсів будується на обладнанні та програмному забезпеченні компаній - лідерів світового ринку телекомунікацій і IT, Cisco (США) і Actility (Франція).

Завдяки такому загальнонаціональному інфраструктурному проекту, Україна повинна вже за рік, перестати бути позаду в розширені прогресу технології Інтернету речей від усього теперішнього світу та стане однією з найбільших центрів досліджень та впроваджень програмних продуктів, необхідного обладнання та дослідження новітніх рішень як для внутрішнього ринку України, так і для ринків усього світу.

Мережі LoRaWAN розгортаються в діапазоні частот, які не потребують ліцензування. Одна базова станція здатна обслуговувати кілька десятків тисяч пристроїв, що обумовлено великим охопленням сигналу і високою завадостійкістю. Крім того, термін служби акумулятора може досягати десяти років. При використанні сонячних батарей пристрій буде працювати автономно до тих пір, поки не закінчиться його ресурс.

Література:

1. Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014) Internet of Things for Smart Cities. IEEE Internet of Things Journal, — 2018. — 22-32 с.

2. D. Bandyopadhyay and J. Sen, "Internet of Things Applications and Challenges in ... Wireless Personal Communications, — 2017. — 49-69 с

ВИКОРИСТАННЯ BIG DATA В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Сеньків Тетяна Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Великі дані - це технологічна можливість, яка змусить центри обробки даних значно трансформуватися та розвиватися. Численні технологічні інновації зумовлюють різке збільшення даних та збору даних. Ось чому великі дані стали останнім напрямком стратегічних інвестицій для IT-організацій. Мета статті це дослідити використання Big Data в інформаційних мережах для прийняття більш ефективних рішень і стратегічних бізнес-кроків.

Величезний обсяг великих даних відкриває еру рішень на основі даних, які будуть формувати мережі зв'язку. Сучасні мережі часто проектуються на основі принципу статичного наскрізного проектування, і їх складність різко зросла за останні кілька десятиліть, що перешкоджає ефективному і інтелектуальному наданню великих даних.

Великі дані (англ. *Big Data*) в інформаційних технологіях — це набори інформації настільки великих розмірів, що традиційні способи та підходи, здебільшого засновані на рішеннях класу бізнесової аналітики та системах управління базами даних, не можуть бути застосовані до них.

Альтернативне визначення називає “Big Data” феноменальним прискоренням нагромадження даних та їх ускладнення.

Для великих даних виділяють традиційні визначальні характеристики, які називаються «Три V» [1, 5]:

а) **Volume** (об'єм) – накопичена база даних охоплює настільки великий обсяг інформації, що його практично нереально обробляти та зберігати традиційними способами.

б) **Velocity** (швидкість) – ця характеристика вказує на швидкість накопичення даних, яка постійно збільшується.

в) **Variety** (різноманітність) – можливість одночасно обробляти структуровану та неструктуровану інформацію.

Big Data працює за принципом чим більшою кількістю інформації ми володіємо, тим точніший прогноз можливо зробити. Також можливість порівняння певних даних та взаємозв'язків між ними дозволяє знайти закономірності, які були приховані до цього. Все це забезпечує глибинне розуміння проблем та, в кінцевому результаті, дозволяє знайти рішення, або можливості керування потрібними процесами.

Найчастіше процес обробки великих об'ємів даних включає в себе побудову моделей та запуск симуляцій [2, 3], під час яких постійно змінюються ключові налаштування, при цьому система постійно відслідковує, як ці зміни впливають на можливий результат. Це все відбувається в автоматичному режимі, допоки не буде знайдено ключовий момент, який допоможе вирішити поставлену задачу.

Оскільки переважна більшість даних є неструктурована, то для перетворення їх у такі, що сприйматимуться людьми, використовуються найсучасніші технології аналізу. До них можна віднести штучний інтелект (AI) та машинне навчання.

Нескінченно великий інформаційний потік, який складає основу Big Data, дозволяє нам отримувати кардинально нові знання, які були недоступні ще кілька років тому. Наприклад, вже зараз проекти, що базуються на Big Data допомагають [4]:

а) Завдяки аналізу величезної кількості медичних записів та обробки медичних знімків можливо точніше і раніше ставити діагнози, краще розуміти природу різноманітних захворювань та винаходити нові ліки та методи лікування.

б) Сільське господарство переживає справжню революцію Big Data, яка допомагає використовувати ресурси так, щоб максимально збільшити врожаї при мінімальному втручанні в екосистему. А також здешевити вирощені продути внаслідок оптимального використання обладнання та добрив.

в) НАСА завдяки аналізу великої кількості даних, отриманих з телескопів, має змогу визначати хімічні склади

атмосфер планет, що знаходяться на відстані багатьох світлових років, та робити припущення про їх придатність для життя.

г) Внаслідок використання нових технологій та аналізу обширних даних з'явилася можливість автоматично попереджувати фінансові махінації з пластиковими картками та відмиванням грошей.

Великі дані мають вагоме практичне значення як технологія, призначена для вирішення актуальних повсякденних проблем, але породжує ще більше нових. Великі дані здатні змінити наш спосіб життя, праці й мислення.

Література:

1. https://rb.ru/howto/chto-takoe-big-data/

2. https://postnauka.ru/faq/46974

3. https://www.datacenterknowledge.com/archives/2015/03/30/big-data-bubble-set-burst

4. http://www.tadviser.ru/index.php/ (Big_Data)

5. https://www.rd-alliance.org/group/big-data-ig-data-development-ig/wiki/big-data-definition-importance-examples-tools

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЇХ ВИКОРИСТАННЯ НА ПІДПРИЄМСТВАХ УКРАЇНИ

Скакун Максим Романович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Постановка задачі. Оскільки інформаційні технології є одним з вирішальних факторів соціально-економічного розвитку, то формування і розвиток інформаційного суспільства повинні бути в центрі уваги сучасних дослідників, а високий рівень актуальності теми зумовлює необхідність її дослідження.

Мета дослідження. Аналіз використання інформаційних технологій на підприємствах України, та їх вплив на формування та розвиток інформаційного суспільства в Україні.

Результати досліджень. Використання сучасних інформаційний технологій (ІТ) на підприємствах є важливою складовою як у формуванні, так і у розвитку інформаційного суспільства в Україні. Під інформаційними технологіями (ІТ) розуміють систему методів і способів збирання, накопичення, зберігання, пошуку та обробки інформації на основі використання засобів обчислювальної техніки [1].

Згідно з визначенням, прийнятим ЮНЕСКО, інформаційна технологія – це комплекс взаємопов’язаних наукових, технологічних, інженерних дисциплін, які вивчають методи ефективної організації праці людей, зайнятих обробкою

і збереженням інформації, обчислювальну техніку і методи організації її взаємодії з людьми і виробничим обладнанням, їх практичні додатки, а також пов'язані з усім цим соціальні, економічні та культурні проблеми.

В Законі України „Про інформацію" інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування [2].

Метою використання інформаційних технологій є ефективне виробництво потрібної інформації для забезпечення ефективного управління ресурсами, створення інформаційного і технічного середовища прийняття раціональних економічних рішень.

З даних визначень можна зробити висновок, що сучасна ІТ спирається на досягнення в області комп'ютерної техніки і засобів зв'язку, а бурхливий розвиток комп'ютерної техніки і інформаційних технологій послужив поштовхом до розвитку економіки, яка побудована на використанні інформації і яка отримала назву інформаційна економіка та є складовим елементом інформаційного суспільства.

Інформаційне суспільство – це суспільство, де всі засоби інформаційної технології, тобто комп'ютери, інтегровані технології, супутниковий і інший зв'язок, відео пристрої, програмне забезпечення, наукові дослідження націлені на те, щоб зробити інформацію загальнодоступною і активно впроваджуваною у виробництво і життя. Основними критеріями інформаційного суспільства є кількість і якість наявної в обігу інформації, її ефективні передача і опрацювання, а також доступність інформації для кожного [3].

Статистична інформація про використання комп'ютерної техніки та телекомунікацій дозволяє оцінити рівень розвитку ІТ в Україні. Згідно даних державної статистики (станом на 09.02.2019 року) було обстежено 49004 підприємств в усіх регіонах України, з яких 44648 (91,1%) підприємств використовували у роботі комп'ютери. Найвищий рівень комп'ютеризації показали підприємства, що здійснювали діяльність у галузі грошового посередництва, надання кредитів, страхування – 99,6% загальної кількості підприємств, які прийняли участь в обстеженні. Найменший рівень комп'ютеризації спостерігався у сфері діяльності готелів та ресторанів – 82,1%. Із загальної кількості підприємств, які

використовували комп'ютери: 62,7% – користувались внутрішньою комп'ютерною мережею, а розширену внутрішню комп'ютерну мережу мало майже кожне шосте підприємство. Кожне четверте підприємство, яке використовувало комп'ютери, мало функціонуючу домашню сторінку у внутрішній комп'ютерній мережі (Інтранет) та використовувало безпровідний доступ для своєї внутрішньої комп'ютерної мережі (рис. 1).

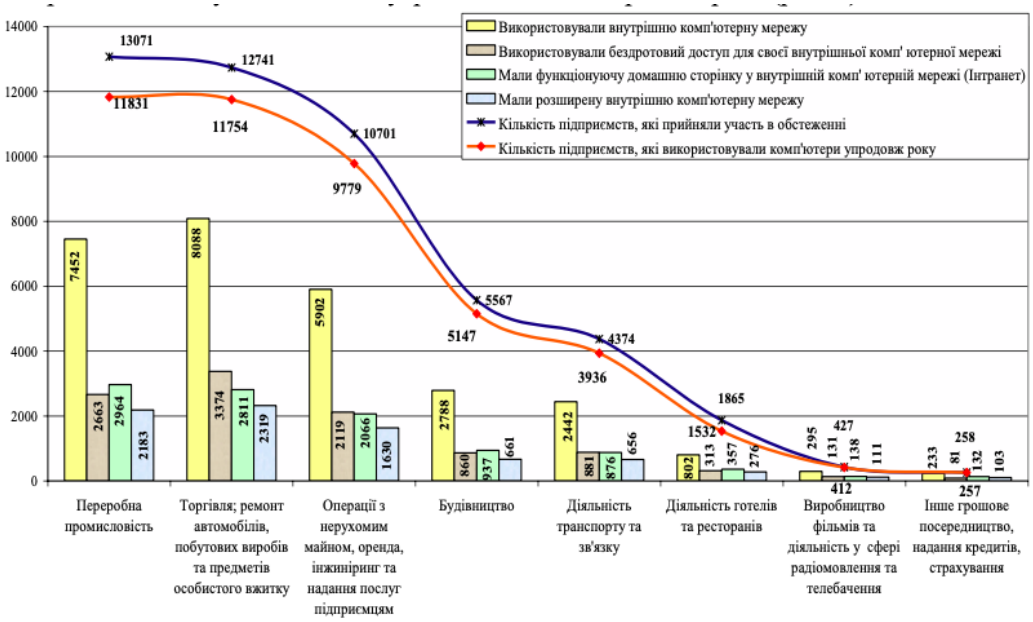


Рис. 1. Використання комп'ютерів та комп'ютерних мереж на підприємствах України станом на 09.02.2019 р.

Питома вага підприємств, що мали доступ до глобальної мережі Інтернет, становила 95,1% (42464 підприємства) загальної кількості підприємств, які використовували комп'ютери. Найбільше поширення мав такий стаціонарний зв'язок з Інтернет, як кабельний, виділена лінія, технологія Frame-Relay або технологія зв'язку лініями електропередачі PLC. Його використовували для роботи 41,1% підприємств, які мали доступ до Інтернет. Кожне третє підприємство для зв'язку з Інтернет застосовувало аналоговий модем (Dial-Up (комутований доступ через телефонну лінію) або зв'язок ISDN (вузькосмуговий) та використовувало широкосмуговий (DSL, xDSL, ADSL, SDSL тощо) Інтернет, майже кожне четверте підприємство зв'язувалось з Інтернет за допомогою мобільного зв'язку (GSM, GPRS, UNTS, EDGE, CDMA2000 1xEVDO, LTE). Підприємства, які мали доступ до Інтернет, використовували його для отримання банківських та фінансових послуг (87,7% підприємств); отримання форм (81,6%); отримання інформації (80,5%); повернення заповнених форм (66,6%); виконання

адміністративних процедур (декларування, реєстрації, запиту на отримання дозволу (40,5%). Більше третини підприємств (39,8%), які мали доступ до Інтернет, вели домашню сторінку або мали Web-сайт. Дві третини підприємств, які на Web-сайті розміщували каталоги продукції або прейскуранти, здійснювали діяльність у переробній промисловості та торгівлі. Кожне четверте підприємство, використовуючи можливості Web-сайту, розміщувало об'яви відкритих вакансій або забезпечувало можливість подач заяв на заміщення вакантних посад у режимі on-line; надавало пропозиції щодо можливості виготовляти продукцію згідно з вимогами клієнта або можливість для клієнтів самостійно розробляти дизайн продукції; здійснювало платежі on-line. Кожне шосте підприємство забезпечувало персоніфіковане інформаційне наповнення в рамках Web-сайту для постійних/повторних клієнтів; розміщувало замовлення або бронювало в режимі on-line [4].

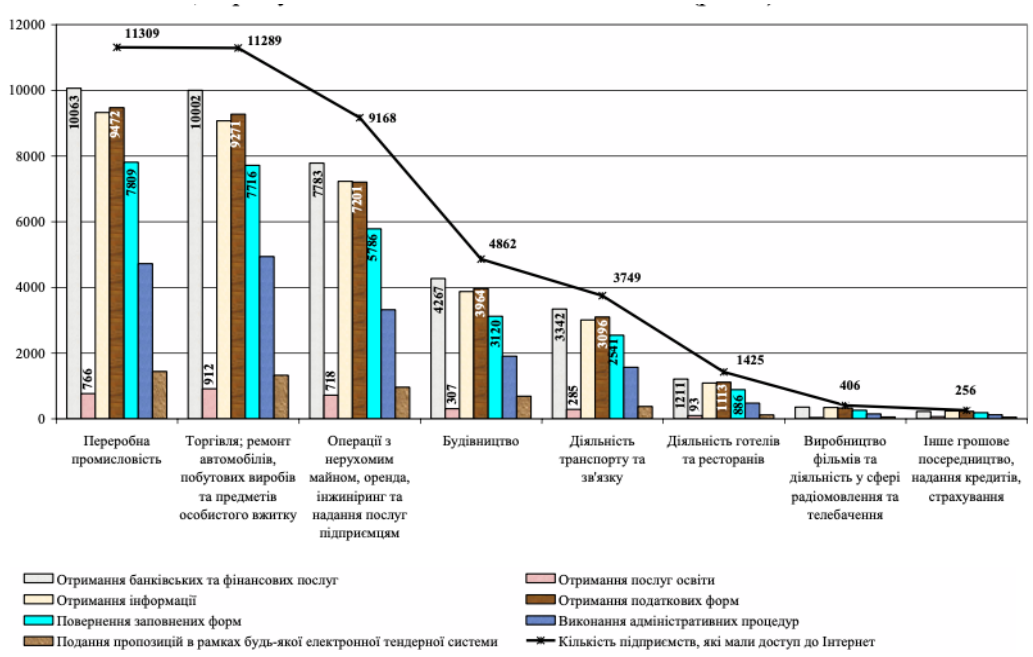


Рис. 2. Напрями використання Інтернету підприємствами України станом на 09.02.2019 р.

Підприємства, які використовували у своїй роботі комп'ютери, активно здійснювали автоматизований обмін даними (відправляли або отримували дані для/від державних установ й транспортну документацію, надавали платіжні доручення фінансовим установам, отримували/відправляли електронні рахунки-фактури, відправляли/отримували інформацію про продукцію, надсилали замовлення постачальникам, отримували замовлення від клієнтів і т.і. (рис. 2).

Всі підприємства (малі, середні та великі) широко використовували можливості Інтернет для отримання банківських та фінансових послуг й інформації взагалі, а також для отримання та повернення заповнених форм. Доступ до Інтернет мали 93,9% малих, 98% середніх та 99,4% великих підприємств.

Органами державної статистики було проведено опитування щодо переваг від використання ІТ, за результатами якого майже у половини респондентів виникли труднощі в оцінці переваг від використання ІТ для покращення роботи у таких напрямках, як виробництво товарів або послуг, управління рівнем технічно- матеріального забезпечення та організація ринків збуту, що є одним із загальновизнаних стримуючих факторів використання ІТ поряд з відсутністю ресурсів для використання ІТ та мотивації у персоналу. У напрямку системи обліку кожен третій респондент відзначив середні або значні

поліпшення від використання ІТ (рис. 3).

Рис. 3. Структура відповідей респондентів щодо усвідомлення переваг від використання ІТ

Висновки. Вітчизняний ринок ІТ перебуває у стані активного становлення та за певних умов повинен стати фундаментом розвитку інформаційного суспільства в Україні. Основною стратегічною метою розвитку інформаційного

суспільства в Україні є прискорення розробки та впровадження новітніх конкурентоспроможних ІТ в усі сфери суспільного життя, зокрема, в економіку України, що дозволить підвищити конкуренто- спроможність України, продуктивність праці у всіх сферах економіки, ступінь розвитку інформаційної інфраструктури, зокрема, українського сегменту Інтернет; збільшити частку наукомісткої продукції; сприяти якості та доступності послуг освіти, науки, культури, охорони здоров'я за рахунок впровадження ІТ; розширити можливості людини отримувати доступ до національних та світових інформаційних електронних ресурсів; створити нові робочі місця, поліпшити умови роботи і життя людини.

Література:

1. Лазарєва С. Ф. Економіка та організація інформаційного бізнесу: навч. посібн. / С. Ф. Лазарєва. – К.: КНЕУ, 2002. – 667 с.

2. Закон України «Про інформацію» від 02.10.1992 No 2657–XII ВР // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi–bin/laws/main. cgi?nreg=2657–12

3. Иноземцев В.Л. К истории становления постиндустриальной хозяйственной системы (1973-2000) // [Електр. ресурс]. - Спосіб доступу: URL:http://scd.centro.ru/rass.htm

4.Використання інформаційно-комунікаційних технологій на підприємствах // Статистичний бюллетень. Державна служба статистики України. – Київ, 2013. – 44 с.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІХ ВИКОРИСТАННЯ В ТУРИСТИЧНОМУ БІЗНЕСІ

Скакун Максим Романович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі. В умовах нашого сьогодення туризм – це глобальний комп'ютеризований бізнес, в якому використовується досить багато новітніх комп'ютерних технологій (напр. глобальні комп'ютерні системи резервування / бронювання, інтегровані комунікаційні мережі, системи мультимедіа, смарт-картки, інформаційні системи менеджменту та ін.) [3] Оскільки інформаційне забезпечення є складовою ресурсного забезпечення, що має вплив на формування туристичного потенціалу території, то потреба у застосуванні найрізноманітніших інформаційних технологій (ІТ) з кожним роком зростає, починаючи від розробки спеціалізованих програмних засобів, що забезпечують автоматизацію роботи окремої туристичної фірми чи готелю, до використання глобальних комп'ютерних мереж. Безумовно, різноманітний асортимент високотехнологічних інформаційних та

комунікаційних технологій вже використовуються у сфері туризму зарубіжними країнами для розробки турпродукту, його реалізації та розповсюдження. З огляду на вищесказане, а також для забезпечення сучасних умов розвитку туристичної індустрії в нашій державі і виникає потреба у підготовці кадрів з інформаційно-технічними знаннями при вільному володінні декількома іноземними мовами, оскільки першоджерела технічної документації – лише англомовні.

Мета дослідження. Метою представленого наукового дослідження є аналіз переваг і недоліків програмних пакетів, визначення сучасної ефективності їх використання у туристичній діяльності, а також розроблення пропозицій щодо можливого їх застосування на підприємствах туристичної галузі.

Результати досліджень. Під час розробки нового туристичного продукту переважна більшість туристичних організацій не можуть обійтися без використання програмних засобів. В сучасних умовах інформатизації та комп'ютеризації швидкий розвиток туристичного бізнесу вимагає нового підходу до обробки інформації та процесу прийняття рішень, тобто необхідно мати конкретний комплекс програмних засобів, а саме: ряд різноманітних алгоритмів підтримки рішень для обґрунтування вибору маршруту, транспортних засобів, місця проживання тощо; бази даних та моделей, що дозволяють створювати можливі варіанти маршрутівта прораховувати найбільш вигідні, здійснювати цінове опрацювання, прогнозувати попит і популярність нових турів, проводити модельний експеримент, що імітує «експериментальний заїзд»; керівну та допоміжні програми [4]. Однак, на сьогоднішній день основний принцип роботиорганізаційних систем в туристичному бізнесі супроводжується процесом генерації великого обсягу інформації та потребує оперативної обробки даних для прийняття рішення, може ускладнюватися цілою низкою чинників, таких як передача неповної, неточної або помилкової інформації, мінливість характеристик і умов функціонування самих систем, наявність людського фактора.

Власне тому переважна більшість фахівців переконана, що успішне функціонування фірми на ринку туристичного бізнесу практично немислимо без використання сучасних ІТ. Специфіка технології розробки та реалізації турпродукту вимагає таких систем, які в найкоротші терміни надаватимуть відомості про доступність транспортних засобів та можливості розміщення туристів, забезпечуватимуть швидке резервування та бронювання місць, а також автоматизацію рішення допоміжних

завдань при наданні турпослуг (паралельне оформлення таких документів, як квитки, рахунки і путівники, забезпечення розрахунковою і довідковою інформацією та ін.) Це доступно за умови широкого використання в туризмі сучасних комп'ютерних технологій для обробки та передачі інформації.

На даний момент в туристично-привабливих частинах Європи вже спостерігається електронний наступ на традиційний туристичний бізнес. Зокрема, на туристичний ринок починає активно проникати і впроваджуватися «електронна комерція» (англ. e-Business). Так, в своїй роботі «eTourism: Information technology for strategic tourism management» професор Дімітріос Бухаліс [10] наголошує на тому, що глобальна мережа Інтернет (або World Wide Web) є ключовою ланкою між туристичними установами, партнерами та клієнтами у спільному використанні інформації, що призвело до організації ділових переговорів на відстані. Таким чином, електронна комерція, що використовується у туристичному бізнесі називається «онлайн-туризм» або «електронний туризм» (англ. e- Tourism). За кордоном вже існують електронні туристичні офіси, наприклад, турбюро «експедитора» фірми Microsoft [3], що дозволяють будь-якому власникові кредитної картки придбати тур, забронювати місцена літак або в готелі, придбати квитки на видовищні заходи і замовити напрокат автомобіль в будь-якій точці земної кулі. Виходячи з вищесказаного можна стверджувати, що пряма розсилка туристичної інформації електронною поштою вже давно не є новаторством, але і досі залишається допоміжним елементом в роботі турфірми.

У вище згаданому дослідженні Дімітріоса Бухаліса [4] детально описано в яких цілях та з якою метою може використовуватись програмне забезпечення (ПЗ) в організаціях туристичного напряму діяльності. Зокрема, туристичні установи / організації в своїй повсякденній роботівикористовують набір прикладних програмних засобів з метою адміністрування та обробки інформації. Наприклад, програмні засоби для обслуговування клієнтів (англ. front-office software) виконують наступний різновид робіт в такому розрізі як реєстрація, підтвердження виїзду, обробка запитів, оформлення замовлень, видача платежів на місці здійснення покупки (касовий термінал), продаж та купівля квитків на проїзд, бронювання туру, складання та планування розкладу. Такі програмні процеси можуть використовувати:

- постачальники турпослуг (англ. Travel Suppliers) – це підприємства, що надають послуги розміщення (напр. готелі, турбази, пансіонати та ін.), підприємства харчування (напр.

ресторани, кафе та ін.), екскурсійні фірми, транспортні компанії, заклади дозвілля (напр. шоу-, кіно-, відео організації), спортивні підприємства, торгові організації та ін.;

- глобальні системи бронювання (англ. Global Distribution Systems), що забезпечують швидке і зручне бронювання квитків на транспорт, резервування місць в готелях, прокат автомобілів, обмін валюти, замовлення квитків на розважальні та спортивні програми;

Провівши аналіз сучасного ПЗ для туристичних підприємств, можна зробити висновок, про те що переважна більшість програм вітчизняного та іноземного виробництва володіє такими функціями, як введення, редагування та зберігання різноманітної інформації про тури, готелі, клієнтів, розклад транспортних засобів в локальних базах даних (в т.ч. можлива експлуатація і віддалених баз даних при наявності встановленого спеціального сервера та програмного забезпечення); розсилка повідомлень електронною поштою (або навіть, SMS- повідомлень) постійним клієнтам про «гарячі» пропозиції і в т.ч. нагадування про виліт / виїзд; статистичний аналіз за різними запитами; багатократне сортування та фільтрування даних за конкретним запитом; підключення до онлайн-постачальників і глобальних систем бронювання за допомогою XML (англ. Extensible Markup Language – «розширена мова розмітки») технологій. Переважно кожна програма має вбудованиймеханізм розширеного та розподільного пошуку: можливість підбору туру за параметрами і бронювання заявок за обраним туром в оператора, здійснює експорт-імпорт даних в інші програмні пакети (Word, Excel, Adobe Reader, бухгалтерські програми: 1С, OPZ), контролює оплату турів, формує фінансову звітність, а також виконує функцію машинного перекладу. Всі вони без винятку дають можливість друкування багато різних документів – від анкет, ваучерів, договорів, списків туристів, листів бронювання до опису готелів, турів тощо. Більшість програмних продуктів дозволяють контролювати оплату турів, друкувати платіжні документи, проводити облік місць у готелі, на транспорті. Однією із важливих функцій подібних програм є також автоматичний розрахунок вартості турів з урахуванням індивідуальних і групових знижок, комісійних, курсів валют та інших чинників.

Висновки і перспективи подальших досліджень. Отже, в роботі узагальнено охарактеризовано основні підходи щодо використання сучасних ІТ в туристичному бізнесі, розкрито суть та роль поняття електронного туризму в туристичній індустрії

спираючись на іноземні джерела. З метою більш детального сприймання та розуміння проблемиздійснено огляд сучасних ІТ-рішень та ПЗ вітчизняного / іноземного виробництва на туристичному ринку. У результаті проведених досліджень запропоновано нові підходи вдосконалення існуючих програмних засобів для обробки туристичної інформації. Сучасні комп'ютерні інформаційні технології здатні кардинально змінювати методичну, інформаційну та технологічну складові управлінських процесів і здійснювати їх на якісно новому, більш ефективному рівні. Однак, в умовах сьогодення все ще існує ряд об'єктивних факторів, що стримують дію на темпи їх впровадження в Україні, до них можна віднести економічну нестабільність, «прогалини» в законодавчому забезпеченні, недостатність освіти управлінських кадрів у сфері ІТ, дефіцит фахівців у галузі інформації, недостатнє державне фінансування науково-дослідних і практичних розробок, пов'язаних з новітніми ІТ, поки що явне відставання, порівняно з іншими країнами, в області розвитку засобів обчислювальної техніки і зв'язку. Поряд з перерахованими проблемами, існує ще маса інших проблем, таких як недостатня компетентність як керівництва всіх рівнів управління підприємством, так і рядових працівників управлінської сфери щодо питань автоматизації (впровадження нових інформаційних систем і технологій); прихильність традиційному підходу у сфері управління. І хоча багато керівників і фахівців розуміють, що час вимагає нових підходів до реалізації більшості завдань, але втілювати їх на практиці не поспішають [3].

Не дивлячись на вище сказане, є надія на те, що комп'ютерні інформаційні технології будуть стрімко еволюціонувати і надалі, даючи поштовх у розвитку науки економічних і управлінських інформаційних технологій та набуваючи все більшої значущості як найважливішого інструмент науково-технічного і соціально-економічного розвитку суспільства. Тобто, результат впровадження комп'ютерних інформаційних технологій – колосальна економія часу фахівців. Відомий вислів «Хто володіє інформацією, той володіє світом» як ніколи актуальний для сфери туристичного бізнесу, для якої характерні такі риси, як оперативність, надійність, точність, висока швидкість обробки і передачі інформації багато в чому визначає ефективність управлінських рішень у цій області.

Література:

1.Лазарєва С. Ф. Економіка та організація інформаційного бізнесу: навч. посібн. / С. Ф. Лазарєва. – К.: КНЕУ, 2002. – 667 с.

2.Закон України «Про інформацію» від 02.10.1992 No 2657–XII ВР // [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi–bin/laws/main. cgi?nreg=2657–12

3.Иноземцев В.Л. К истории становления постиндустриальной хозяйственной системы (1973-2000) // [Електр. ресурс]. - Спосіб доступу: URL:http://scd.centro.ru/rass.htm

4.Використання інформаційно-комунікаційних технологій на підприємствах // Статистичний бюллетень. Державна служба статистики України. – Київ, 2013. – 44 с.

ЩО ТАКЕ ІНТЕРНЕТ РЕЧЕЙ?

Слівенко Анастасія Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У сучасному суспільстві основним технічним засобом технології переробки інформації служить ПК, який істотно вплинув як на концепцію побудови і використання технологічних процесів, так і на якість результатної інформації.

Впровадження ПК в інформаційну сферу та застосування телекомунікаційних засобів зв'язку визначили сучасний етап розвитку ІТ. У поняття сучасної ІТ включені також комунікаційні технології, які забезпечують передачу інформації різними засобами, а саме - телефон, телеграф, теле-комунікації, факс та ін.

Завдяки широкому розповсюдженню комп'ютерів і створення Інтернету люди можуть спілкуватися між собою через ПК. Для більшості Інтернет це поширена і звична глобальна мережа, яка вже використовується як звичайні спосіб в отримання, передачі інформації. За допомогою Інтернету, комп'ютер стає справжнім засобом зв'язку. Кожен, хто має доступ до WWW, може отримати всю необхідну йому інформацію, а також передати її по всьому світу. Зараз саме Інтернет робить роботу, бізнес більш ефективним, ніж раніше, тому що люди мають широкий доступ до отримання будь-якої інформації, про що раніше не можна було сказати.

Особливості сучасних ІТ:

− Робота користувача в режимі маніпулювання (без програмування) даними. Користувач не повинен знати і пам'ятати, а повинен бачити (пристрої виведення) і діяти (пристрої введення).

− Наскрізна інформаційна підтримка на всіх етапах проходження інформації на основі інтегрованої БД, яка передбачає єдину форму введення, пошуку, відображення, відновлення і захисту інформації.

− Безпаперовий процес обробки документа, під час якого на папері фіксується тільки його остаточний варіант, а проміжні версії і необхідні дані, записані на носіях, поставляються користувачеві через екран дисплея ПК.

− Інтерактивний режим рішення задач з широкими можливостями для користувача.

− Колективне виготовлення документа на основі групи ПК, об'єднаних засобами комунікації.

− Адаптивна переробка форми і способів подачі інформації в процесі виконання завдання.

Нижче перераховані сучасні ІТ, найбільш часто використовувані в системах різного типу і призначення.

Сучасні ІТ:

− математичне і комп'ютерне моделювання;
− БД і знань;
− експертні та інтелектуальні системи;
− кошти, технології планування та управління за допомогою електронних таблиць;
− електронна пошта і телекомунікаційні засоби;
− інтегровані пакети прикладних програм і середовища;
− кошти, методи і технології машинної графіки та анімації;
− кошти, методи і технології мультимедіа;
− гіпертекстові технології і WWW-технології;
− CASE-технології та ін.

Формування та вдосконалення інформаційних технологій є одним з головних чинників в суспільстві. Поширення ІТ перетворює життя людей, полегшує роботу, дає більше вільного часу, приносить розвиток в економічній, культурній, освітній та інших сферах.

Сучасне суспільство наповнене і пронизане потоками інформації, які потребують обробки. Тому без інформаційних технологій, так само як без енергетичних, транспортних і хімічних технологій, воно нормально функціонувати не може.

Література:

1.https://www.sviaz-expo.ru/ru/articles/sovremennye-informacionnye-tehnologii/
2.https://works.doklad.ru/view/GRx9bTCcRpY.html

SSL-СЕРТИФІКАТ

Сліпець Артем Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій

Багато хто думає, що безпека в Інтернеті – це ілюзія, і бути захищеним зараз неможливо, адже веб-сайти збирають конфіденційну інформацію так тонко, що ми навіть не знаємо що саме їм відомо. Це, можливо, й так, але ця невпевненість – ще одна причина, щоб зберегти свою приватність та уникнути витоку персональних даних в Інтернет.

SSL сертифікат це цифровий підпис Вашого сайту, його призначення в тому щоб обмін даними між Вашим сайтом і браузером клієнта здійснювався по захищеному каналу зв'язку. Всі дані будуть передаватися в зашифрованому вигляді зі спеціальним цифровим підписом. Тому сайти які використовують SSL викликають більше довіри у відвідувачів.

На деяких сайтах біля адреси сторінки в браузері відображається значок замка. Він буває зеленого, золотого або сірого кольору. Буває, замок перекреслений або взагалі відсутній, а іноді поряд з доменним ім'ям з'являється зелений рядок з назвою компанії.

Замок або зелений рядок означають, що на сайті встановлений SSL-сертифікат і вся інформація передається по захищеному протоколу. Протокол - це такий набір правил. Браузер і сервер використовують його, щоб обмінюватися інформацією.

SSL-сертифікат не дає шахраям перехопити або підмінити особисті дані користувачів: контактну інформацію, номери банківських карт, логіни, паролі, адреси електронної пошти і т.д.

SSL сертифікати бувають трьох видів:

1. «Самоподпісаний» сертифікати (Self-Signed SSL). Це означає, що ви самостійно зробили для себе цей SSL сертифікат.
2. Підписано не довіреним центром сертифікації (Self-Signed SSL). Це означає, що сертифікат перевірений, але виданий він не довіреним центром сертифікації.
3. SSL сертифікат виданий довіреним центром сертифікації (Trusted SSL). Це означає, що сертифікат виданий сертифікованою компанією, що займається видачею сертифікатів.

При використанні «самоподпісанного» сертифікату більшість браузерів при першому зверненні інформують користувача сайту про це, і надалі, як правило, позначають такий сайт спеціальним значком. Такий варіант безумовно піднімає рівень захисту сайту, але варто його використовувати для закритої частини сайту, доступ до якої мають тільки співробітники компанії. Trusted SSL видається спеціалізованими центрами сертифікації та гарантує високий ступінь захисту вашого сайту. Браузери позначають звернення до таких сайтів

спеціальним значком і довіряють такому з'єднанню. При зломі таких SSL сертифікатів відповідальність лежить тільки на центрі сертифікації .

За підтримкою кількості доменів сертифікати поділяються на:

1. Standard (стандартні)

2. WildCard (групові)

Standard сертифікат формується для захисту тільки одного домену, без субдоменів. Якщо такий сертифікат буде підключений на інший домен або на піддомен того домену, якому він був виданий, браузер повідомить про помилку. Приміром якщо сертифікат виданий для domain.com, броузер буде довіряти https://domain.com, але при зверненні до https://www.domain.com буде сигналізувати про помилку.

WildCard сертифікат. Це сертифікат для домену та всіх його піддоменів. Такий сертифікат виглядає як *. Domain.com і його можна використовувати як для https://domain.com так і для https://test.domain.com

Література:

1. *https://ssl.com.ua/info/what-is-ssl/*
2. *https://freehost.com.ua/faq/faq/scho-take-ssl-sertifikat-i-navischo-vin-potriben/*
3. *https://ua.godaddy.com/help/sho-take-sertifikat-ssl-542*
4. *https://pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbno-znati.html*

NFC (NEAR FIELD COMMUNICATION)

Сліпець Артем Сергійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Оплачувати будь-які покупки, не використовуючи при цьому готівки, сьогодні простіше, ніж коли-небудь. Для цього навіть не обов'язково діставати свою кредитку з гаманця. Система NFC дозволяє зробити це, не торкаючись до терміналу, а просто піднісши картку, смартфон, годинник або інший пристрій на певну відстань від нього. Унікальна методика стрімко набирає популярність у всьому світі, оскільки виводить придбання товарів на абсолютно новий за зручністю рівень.

Технологія безконтактних платежів відома як NFC - Near field communication. Переклад - «ближній зв'язок без контакту». Розберемо кожне слово, щоб краще зрозуміти як влаштована технологія.

Термін «ближній» означає, що Ваша інформація може відбуватися на невеликій відстані технічних пристроїв один від одного. Відстань не перевищує чотирьох сантиметрів.

Значення слова «без контакту» полягає в тому, що відносини не вимагає прямого впливу картки на торговий термінал. Зчитування даних відбувається за допомогою індукції магнітного поля. Слово «зв'язок» теж вельми зрозуміло і логічно і позначає взаємодію між двома технічними засобами.

Таким чином, виходить, що система NFC - це обмін даними між 2 пристроями, що відбувається з використанням принципу магнітного впливу. Це визначення не розкриває всю сутність технології, але демонструє головні її риси.

NFC є прямим конкурентом вже звичної для нас технології Bluetooth. Суттєва перевага NFC над Bluetooth - це швидкість з'єднання між двома пристроями. З'єднання пристроїв відбувається швидше, ніж за одну десяту секунди. А для «конекту» пристроїв по Bluetooth вам потрібно узгоджувати з'єднання на двох апаратах окремо. До того ж, менший радіус дії робить дану технологію безпечнішою.

Що стосується ринку мобільних пристроїв, то дана технологія найчастіше використовується тільки для двох речей: передача файлів на інший пристрій і оплата покупок / послуг. Наприклад, завдяки NFC-чіпом у вас є можливість оплатити покупку в магазині без своєї банківської картки. Передача файлів стала можлива після того, як пошуковий гігант Google анонсував Android 4.0 Ice Cream Sandwich, в якому дебютувала функція Android Beam. Більш того, підтримка пристроєм технології Near Field Communication дозволяє йому зчитувати або записувати програмовані NFC-мітки.

Переваг у технології дуже багато, інакше вона не стала б так активно розвиватися і поширюватися. Серед іншого її цінують за:

1. Можливість швидкого проведення операцій.
2. Відсутність необхідності давати свою карту в руки чужої людини.
3. Високу технологічність.
4. Зручність і комфорт при здійсненні покупок.

Мінуси теж є, але з часом їх стає все менше. Найважливішим з них можна вважати невелику кількість торгових точок, чиє обладнання підтримує NFC. З цим недоліком борються самі фінансові установи, які є еквайєрами для магазинів. Поступово вони замінюють термінали на нове обладнання, в якому з легкістю можна користуватися послугою.

Ще однією проблемою, з якою реально зіткнутися, є досить висока ціна на торгове обладнання, що підтримує безконтактні картки. Особливо сильно це заважає власникам

невеликих підприємств торгівлі. Але і вони при більш ретельному розгляді питання нерідко змінюють свою думку.

У кредитки вбудовується внутрішній чіп, що випромінює радіохвилі через антену, ті самі, які розпізнаються технологією RFID. Сам термінал при цьому оснащується зчитувачем, уловлює дані.

Коли клієнт підносить свій «пластик» до торгового обладнання на невелику відстань, сигнал з носія зчитується, і обробляються ідентифікаційні дані. При цьому маленькі суми покупки не вимагають, взагалі, ніяке додаткове підтвердження, для великих необхідно вводити пін-код.

Тримати картку у банківського терміналу потрібно протягом пари секунд. Цього часу було достатньо, щоб отримати всі необхідні відомості і передати їх в еквайринговий центр. Щоб покупець точно знав, коли можна прибирати платіжний інструмент, пристрій видає звуковий сигнал.

Література:

1. *https://blog.allo.ua/chto-takoe-nfc_2017-09-38/*
2. *https://f.ua/ua/articles/chto-takoe-nfc.html*
3. *https://www.cleverence.ru/articles/elektronnaya-kommertsiya/beskontaktnaya-oplata-chto-eto-takoe-funktsii-tekhnologii-kak-rabotaet-sistema-i-kak-ey-polzovatsya/*

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВОГО КОМП'ЮТЕРА

Смірнов Владислав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Що таке квантові обчислення?

Квантові комп'ютери можуть стимулювати розвиток нових проривів у науці, ліки для порятунку життя, методи машинного навчання для швидшої діагностики захворювань, матеріали для виготовлення більш ефективних пристроїв та конструкцій, фінансові стратегії для доброго життя на пенсії та алгоритми для швидкого спрямування таких ресурсів, як машини швидкої допомоги.

Але що саме таке, ці квантові обчислення, і що потрібно для досягнення квантових проривів? Ось, що потрібно знати.

1. Новий вид обчислень

Ми відчуваємо переваги класичних обчислень щодня. Однак існують проблеми, які сучасні системи ніколи не зможуть вирішити. Для проблем, які перевищують певний розмір і

складність, на Землі нам не вистачає обчислювальних потужностей для їх вирішення.

Щоб мати шанс вирішити деякі з цих проблем, нам потрібен новий вид обчислень. Універсальні квантові обчислювальні машини використовують квантово-механічні явища суперпозиції та переплутування для створення станів, які масштабуються експоненціально з кількістю кубітів або квантових бітів.

2. Основи квантових обчислень

Усі обчислювальні системи покладаються на фундаментальну здатність зберігати та маніпулювати інформацією. Нинішні комп'ютери маніпулюють окремими бітами , які зберігають інформацію у вигляді двійкових станів 0 та 1. Квантові комп'ютери використовують квантово-механічні явища для маніпулювання інформацією. Для цього вони покладаються на квантові біти або кубіти.

3. Всередині квантового комп'ютера

Існує кілька різних способів створити кубіт. Один метод використовує надпровідність для створення та підтримання квантового стану. Щоб працювати з цими надпровідними кубітами протягом тривалого періоду часу, вони повинні бути дуже холодними. Будь-яке нагрівання в системі може спричинити помилку, саме тому квантові комп’ютери працюють при температурах, близьких до абсолютного нуля, холодніших, ніж вакуум космосу.

4. Загляньте всередину квантового комп’ютера

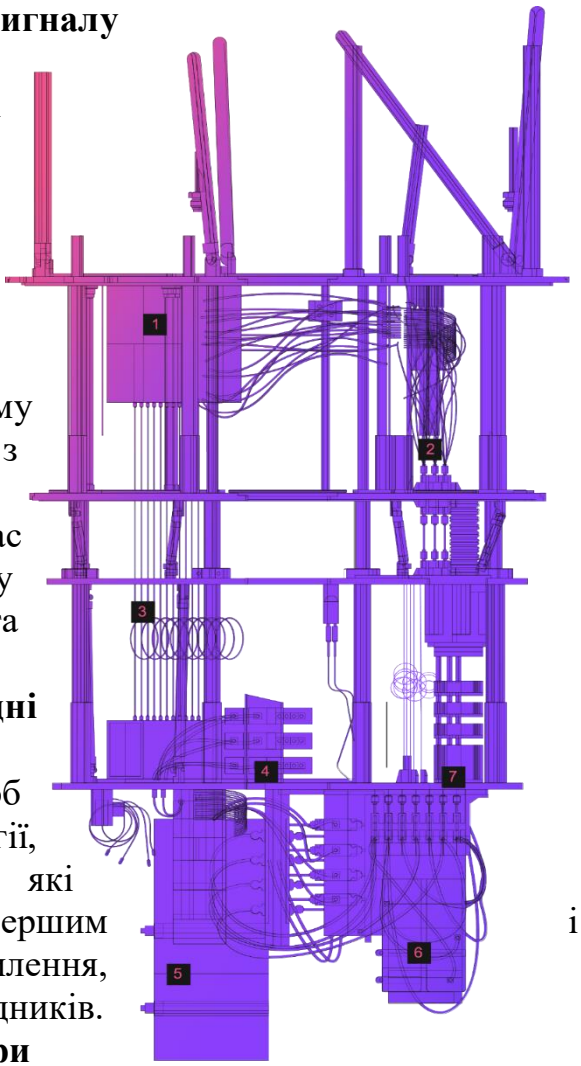
Погляньте на те, як холодильник квантового комп’ютера, виготовлений з понад 2000 компонентів, використовує властивості змішування двох ізотопів гелію, щоб створити таке середовище для кубітів всередині.

1. **Підсилювач сигналу Qubit**

Одну з двох ампліфікаційних стадій охолоджують до температури 4 Кельвіна.

2. **Вхідні мікрохвильові лінії**

Ослаблення застосовується на кожному етапі в холодильнику з метою захисту кубітів від теплових шумів під час надсилання процесору сигналів керування та зчитування.



3. **Надпровідні коаксіальні лінії**

Для того, щоб мінімізувати втрати енергії, коаксіальні лінії, які направляють сигнали між першим і другим каскадами підсилення, виготовляються із надпровідників.

4. **Кріогенні ізолятори**

Кріогенні ізолятори дозволяють сигналам кубітів рухатись вперед, одночасно запобігаючи шуму, що порушує якість кубіта.

5. **Квантові підсилювачі**

Квантові підсилювачі всередині магнітного екрану захоплюють і посилюють сигнали зчитування процесора, мінімізуючи шум.

6. **Щит кріоперми**

Квантовий процесор знаходиться всередині екрану, який захищає його від електромагнітного випромінювання, щоб зберегти його якість.

7. **Змішувальна камера**

Змішувальна камера в нижній частині холодильника забезпечує необхідну потужність охолодження, щоб знизити процесор та супутні компоненти до температури 15 мК - холоднішої, ніж космічний простір.

Література:

1. *https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/*
2. *https://habr.com/ru/company/ua-hosting/blog/377533/*

ЩО ТАКЕ ІНТЕРНЕТ РЕЧЕЙ?

Смірнов Владислав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Від щіток для волосся до ваг, споживчі та промислові пристрої мають вбудовані мікросхеми для збору та передачі даних

Розумні тостери та фітнес-нашийники для собак - це лише деякі з повсякденних "німих предметів", які підключаються до Інтернету як частина Інтернету речей (IoT).

Підключені машини та предмети на фабриках відкривають потенціал для четвертої “промислової революції”, експерти прогнозують, що більше половини нових підприємств працюватимуть на IoT до 2022 року.

Ось усе, що вам потрібно знати про світ, який дедалі більше пов’язується.

Що таке Інтернет речей?

У найширшому розумінні термін IoT охоплює все, що пов’язано з Інтернетом, але він все частіше використовується для визначення об’єктів, які «розмовляють» між собою. "Просто Інтернет речей складається з пристроїв - від простих датчиків до смартфонів та носіїв - пов'язаних між собою" , - говорить Метью Еванс, керівник програми IoT в techUK

Поєднуючи ці підключені пристрої з автоматизованими системами, можна «зібрати інформацію, проаналізувати її та створити дію», щоб допомогти комусь із певним завданням або навчитися з процесу. Насправді це варіюється від розумних дзеркал до маяків у магазинах та за його межами.

"Йдеться про мережі, про пристрої та про дані", - пояснює Керолайн Горський, керівник Інтернету речей у Digital Catapult. IoT дозволяє пристроям, що перебувають у закритому приватному Інтернет-з'єднанні, спілкуватися з іншими, і "Інтернет речей зближує ці мережі. Це дає можливість пристроям спілкуватися не лише в тісних шахтах, але через різні типи мереж і створює набагато більш пов'язаний світ".

Чому підключеним пристроям потрібно обмінюватися даними?

Було піднято аргумент, що лише те, що щось можна підключити до Інтернету, не означає, що це повинно бути, але

кожен пристрій збирає дані з певною метою, які можуть бути корисними для покупця та впливати на економіку в цілому.

У промислових цілях датчики на товарних лініях можуть підвищити ефективність та зменшити кількість відходів. Одне дослідження підрахувало, що 35 відсотків американських виробників вже використовують дані інтелектуальних датчиків у своїх установках. Американська фірма Concrete Sensors створила пристрій, який можна вставити в бетон, наприклад, для надання даних про стан матеріалу.

"IoT пропонує нам можливість бути ефективнішими в тому, як ми робимо щось, заощаджуючи нам час, гроші та часто викиди в процесі", - говорить Еванс. Це дозволяє компаніям, урядам та державним органам переосмислити, як вони надають послуги та виробляють товари.

"Якість та обсяг даних у Інтернеті речей створює можливість для набагато більш контекстуалізованих та реагуючих взаємодій з пристроями, щоб створити потенціал для змін", - продовжив Горський. Це "не зупиняється на екрані".

Куди далі йде IoT?

Навіть ті, хто придбав один з безлічі розумних товарів для дому - від лампочок, перемикачів до датчиків руху - підтвердять факт того, що IoT перебуває в зародковому стані. Продукти не завжди легко з’єднуються між собою, і є серйозні проблеми безпеки, які потрібно вирішити.

У звіті Samsung йдеться про необхідність захистити кожен підключений пристрій до 2021 року "критично важливо". У документі фірми "Відкрита економіка" сказано, "існує цілком очевидна небезпека того, що технології випереджають гру". Компанія заявила, що до 2021 року їх виробники повинні забезпечити безпеку понад 7,3 мільярда пристроїв.

"Ми дивимось у майбутнє, в якому компанії будуть віддаватися цифровому дарвінізму, використовуючи IoT, AI та машинне навчання, щоб швидко розвиватися так, як ми ніколи раніше не бачили", - сказав Брайан Соліс з Altimeter Group, який допомагав у дослідженні. .

IoT-ботнети, створені з використанням мережі застарілих пристроїв, у 2016 р. Великі веб-сайти та служби перестали працювати в режимі офлайн . Китайська фірма згодом відкликала 4,3 млн. Незахищених підключених камер. Легкість збиття Інтернету за допомогою пристроїв IoT виявилася, коли замість шкідливих цілей виявилося, що ботнет створений для гри Minecraft .

Але чи немає наслідків для конфіденційності?

Все, що підключено до Інтернету, можна зламати, продукти IoT не є винятком із цього неписаного правила. Небезпечні системи IoT призвели до того, що виробник іграшок VTech втратив відео та фотографії дітей за допомогою підключених пристроїв.

Також є питання спостереження. Якщо кожен продукт стане зв'язаним, тоді існує можливість нестримного спостереження за користувачами. Якщо підключений холодильник відстежує споживання та споживання їжі, винос може бути націлений на голодних людей, які не мають їжі. Якщо розумний годинник може виявити, коли ви займаєтесь сексом, що зупинить людей, які користуються цими даними, проти власника годинника?

"У майбутньому спецслужби можуть використовувати [Інтернет речей] для ідентифікації, спостереження, моніторингу, відстеження місцезнаходження та націлювання для вербування або для отримання доступу до мереж або облікових даних користувачів", Джеймс Клаппер, американський напрямок або національна розвідка заявив у 2016 році. Wikileaks пізніше заявив, що ЦРУ розробляє аналітику безпеки для підключеного телевізора Samsung.

Нам потрібні надійні стандарти

У центрі створення величезної, надійної мережі IoT лежить одне важливе питання: сумісні стандарти. Об'єднані об'єкти повинні мати можливість розмовляти між собою, щоб передавати дані та ділитися записаним. Якщо всі вони працюють за різними стандартами, вони намагаються спілкуватися та ділитися. Інститут асоціації електричних та електронних стандартів перелічує величезну кількість стандартів, що розробляються та працюють над різними програмами.

"З'являються додаткові потреби у стандартизації", - каже Інтернет-товариство . Якщо стандартизація відбудеться, це дозволить підключати більше пристроїв та додатків.

Щоб спробувати вирішити цю проблему в масштабах підприємства, Microsoft представила власну систему для пристроїв IoT. Під назвою IoC Central, TechCrunch повідомляє, що система надає компаніям керовану центральну платформу для налаштування пристроїв IoT. Microsoft стверджує, що система буде просто створювати мережі IoT.

Горський описав IoT, навіть серед тих, хто має найбільший досвід концепції, як "відносно незрілий ринок", але сказав, що 2016 рік може стати переломним. Стандарт Hypercat зараз підтримується ARM, Intel, Amey, Bae Systems та Accenture,

і в даний час фірми домовляються про формат "виставлення колекцій" URL-адрес, наприклад.

"У короткостроковій перспективі ми знаємо, що [IoT] впливатиме на все, де є велика вартість невтручання", - сказав Еванс. "І це буде стосуватися простих повсякденних питань, таких як пошук місця для паркування автомобілів у жвавих районах, підключення домашньої розважальної системи та використання веб-камери холодильника, щоб перевірити, чи потрібно вам більше молока по дорозі додому.

"Зрештою, захоплюючим є те, що ми ще не знаємо точних випадків використання, і просто те, що це може мати великий вплив на наше життя".

Література:

1. *https://www.ibm.com/quantum-computing/learn/what-is-quantum-computing/*
2. *https://habr.com/ru/company/ua-hosting/blog/377533/*

ПОЄДНАННЯ МЕТОДІВ TDD ТА BDD ДЛЯ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ВНУТРІШНЬОГО ТЕСТУВАННЯ

Соколовський Ян Вадимович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

У даній статті розглядається процес розробки програмного забезпечення та аналізується важливість етапу тестування, адже це є важливим кроком для виявлення помилок. В роботі порівнюється використання комбінації таких двох різних методів тестування як "Тестова розробка" (TDD) та "Поведінкова розробка" (BDD). Варто зазначити, що метод тестування TDD — це процес із великим відсотком коду, який перевіряється автоматично, однак, саме це може призвести до помилки при зміні параметрів функцій. На противагу метод тестування BDD - це метод тестування, який може успішно працювати, незважаючи на зміни параметрів функцій.

Як результат, в даній роботі нами було розглянуто поєднання методів тестування TDD та BDD, яке називається методом T-BDD.

Вступ

В сучасному світі, розробляючи програмні систему чи додаток, значна кількість розробників програмного забезпечення дотримуються ряду важливих конкретних етапів, котрі відомі під назвою "Методології розробки програмного забезпечення" [1, с.86-94] . Існує безліч прикладів таких методологій, як наприклад Agile, Water Fall, Lean Development та багато інших, які застосовуються як орієнтири для процесу розробки програмного забезпечення. Для будь-якої методології розробки програмного забезпечення етап тестування відіграє важливу роль у створенні надійного програмного забезпечення, у виявленні будь-яких помилок, які можуть виникнути на етапах

розробки, а також у забезпеченні якості та продуктивності продукту [2].

Існує багато методів тестування програмного забезпечення [3]. Як вже було зазначено вище, у цій роботі розглядається використання та поєднання методів тестування TDD та BDD для тестування внутрішньої системи. Ці методи тестування були застосовані в процесі розробки серверної системи для платформи веб-додатків Vixio. При обслуговуванні повністю функціонального коду внутрішньої системи Vixio різні речі всередині системи час від часу вимагають доопрацювання, включаючи якість коду та методи тестування. Для модульного тестування серверної системи Vixio застосовуть метод тестування TDD. Етапи тестування були показані з самого початку створення нової функції, наприклад, визначення цілі, створення модульного тесту та написання коду, поки модульний тест не виявив помилок або збоїв. Незважаючи на те, що охоплення тестом коду було високим, все ще існувала проблема з використанням методу тестування TDD. Проблема сталася в момент, коли значення параметрів функції були змінені, внаслідок чого тестова функція стала схильною до помилок, а тому тестова функція потребувала оновлення або переписування. Для вирішення даної проблеми TDD у цьому сценарії тестування бекенда було використано метод тестування BDD застосовується в тестовій функції. Метод тестування BDD — це тести поведінки програми, а не реалізації. Це означає, що вхідні та вихідні дані стали динамічною формою відповідно до сценарію програми. Отже, поєднуючи методи тестування BDD і TDD, це, сподіваємось, може надати доказ того, що такі два методи тестування можуть доповнювати один одного і давати найкращий результат одиничного тесту для внутрішньої системи Vixio. поєднання методів тестування TDD та BDD, що стосується тестування T-BDD, у внутрішній системі Vixio.

Теоретична основа

Бекенд-система Vixio. Як уже згадувалося раніше, для застосування методу тестування T-BDD, для об'єкта тестування використовувалася бекенд-система Vixio. Vixio - це платформа веб-додатків, яка забезпечує інтерактивне середовище, яке дозволяє користувачам писати інтерактивні історії, а також ділитися ними з читачами для відтворення. Бекенд Vixio був розроблений з використанням фреймворку Laravel. Laravel — це фреймворк з відкритим кодом, який використовує PHP як мову програмування. Структура Laravel забезпечує такі модулі, як автентифікація, маршрутизація, сеанси та кешування, які зазвичай використовуються для веб-додатків. Laravel також

надає підтримку для тестування за допомогою PHPUnit [4, с. 247-64]. Тестування включає JSON API для перевірки JSON та тестування завантажених файлів. PHPUnit може допомогти розробнику протестувати та налагодити кожну кінцеву точку, створену у вигляді модульного тесту. Модульний тест використовується, щоб допомогти розробнику розробити свій код, зберігаючи при цьому код захищеним від помилок та помилок під час внесення змін.

Тестова розробка. Тестова розробка (TDD) — це метод тестування, який зобов'язує розробника встановити цілі тесту перед початком написання коду. Після створення тесту розробник повинен написати код, щоб задовольнити тест, доки не буде помилок. Етапи методу тестування TDD можна побачити на рисунку 1 нижче:

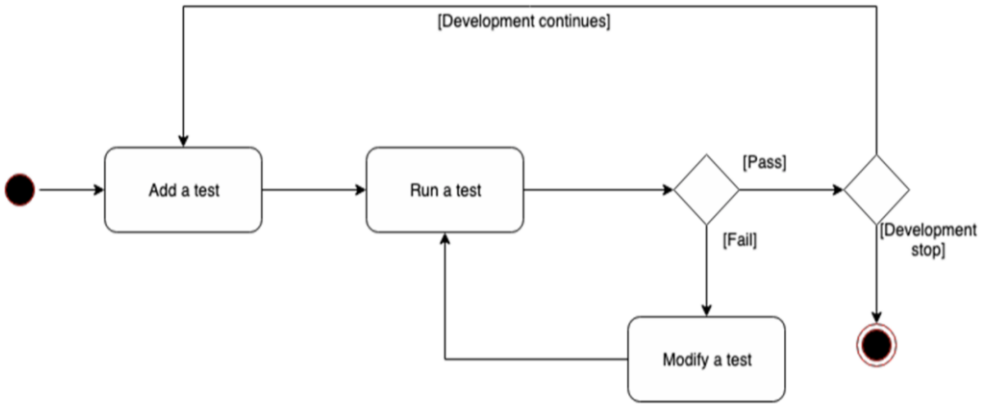


Рис. 1

Процес використання TDD полягає в наступному: (1) встановити мету для нової функції та застосувати її до тестової функції; (2) запустити тест, який призводить до помилок або збоїв; (3) Напишіть код для цієї тестової функції; (4) повторно запустити функцію тестування. Якщо результат показує помилку, повторіть третій крок і рефакторингуйте код, поки помилки не буде знайдено; та (5) повторювати процес TDD для нової функції, поки не буде більше функцій.

Проблема використання методу тестування TDD полягає в тому, що розробнику потрібно подумати, що слід записати в тестовій функції, коли тестувати нічого. Однак, п’ять порад, які можуть допомогти розробникам, які легше використовують метод тестування TDD, — це (1) визначити вхідні та вихідні дані для цієї конкретної функції; (2) визначити параметри всередині тестової функції; (3) розділити аспекти ознаки та зосередитись на аспекті один за одним; (4) реалізувати функцію тестування, думаючи про поведінку коду, а не про реалізацію коду; та (5) реалізувати код, завдяки якому аспекти передаються по одному.

Поведінкова розробка. Поведінкова розробка (BDD) — це метод тестування, який фокусує тест на основі сценаріїв або особливостей (поведінки) реалізованого коду замість процесу реалізації коду. Метод тестування BDD забезпечує такі переваги, як (1) проста організація функції тестування; (2) більш точні та ефективні для використання позначень, обміну знаннями та організації бесіди між розробниками; та (3) не потрібно змінювати функції тесту, незважаючи на вимоги зміни коду. На рисунку 2 показано порівняння між традиційними етапами спринту та етапами спринту з повною поведінкою(BDD)

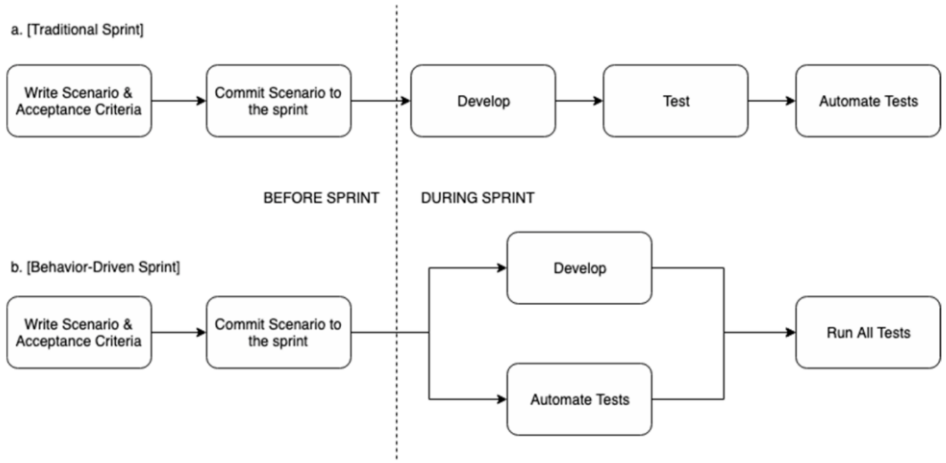


Рис. 2

Виходячи з цих переваг, BDD — це дуже зручний метод тестування, який можна реалізувати в динамічних сценаріях. Він вирішує проблему, показуючи, як проводити тестування. Отже, замість того, щоб думати про те, як реалізований код, розробник повинен подумати, з якими сценаріями зіткнеться код. Для того, щоб зрозуміти етапи методу тестування BDD, сценарій або дизайн поведінки може змусити розробника підготувати кращий тест для методу тестування BDD [5].

Розробка заснована на тестовій поведінці (T-BDD). З метою вдосконалення методу тестування розробленої внутрішньої системи для Vixio, ця робота — це спроба поєднати методи тестування TDD у спринт BDD під назвою T-BDD. На підставі попередніх пояснень щодо TDD та BDD вище, TDD підтримує процес розробки шляхом визначення етапу тестування. Поєднуючи цей метод із BDD, передбачалося, що процес розробки все ще може бути протестований за різними сценаріями. Тут усі заздалегідь визначені функції модульного тесту для TDD були включені в процес розробки, де було визначено та зафіксовано функцію сценарію та поведінки серверної системи. Загалом, конструкцію комбінації при

формуванні методу тестування T-BDD можна побачити на рисунку 3.

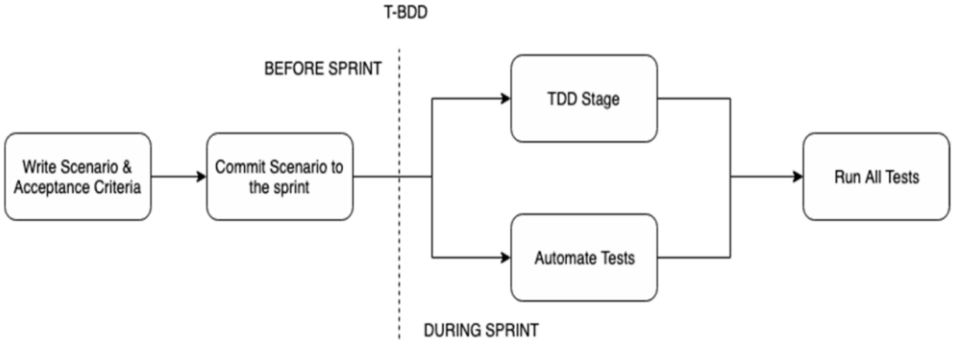


Рис. 3

Архітектура системи

Структура Laravel була використана для створення внутрішньої системи Vixio, вона включає систему управління вмістом (CMS) та інтерфейс програмування додатків (API). За допомогою маршрутів Laravel користувачі створювали та використовували кінцеві точки для API та CMS. На рисунку 4 показана архітектура серверної мережі Vixio:

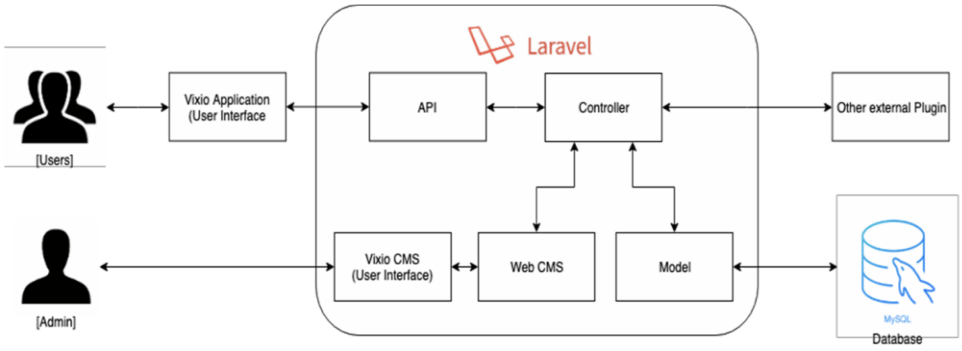


Рис. 4

Функції, розташовані в контролері з певними операціями, запускаються за допомогою виклику кінцевої точки API. Функції виконують запити з використанням Eloquent Library, від Laravel. Виконані запити обробляються в моделі, що підключена до бази даних. Потім функції повертають результат і надають відповідь користувачам. Розробка користувальницького інтерфейсу Vixio CMS використовує шаблони блейдів, надані Laravel. Цей користувальницький інтерфейс пов'язаний з веб-маршрутом, що дозволяє користувачам отримувати доступ до зареєстрованих кінцевих точок, створених маршрутом, що спрямовує браузер користувача до вказаних сторінок леза. Перш ніж направляти користувача, буде активована функція з кінцевої точки, до якої здійснюється доступ. Для веб-маршруту запит на метод POST HTTP вимагав підробки міжсайтового запиту (CSRF) маркер. Цей запит було передано контролеру, коли

маркер був перевірений проміжним програмним забезпеченням “VerifyCsrfToken”, що надається Laravel. У цій системній архітектурі API надає кінцеві точки, до яких користувачі можуть отримати доступ для створення вихідних даних у форматі JSON. Вихід забезпечується функцією, яка запускається кінцевою точкою, до якої здійснюється доступ. Доступні кінцеві точки реєструються в маршруті Laravel API. На відміну від веб-маршрутів, які вже надаються з верифікацією маркера CSRF, маршрут API вимагає інших методів перевірки маркерів у проміжному програмному забезпеченні. Для автентифікації серверна система використовує веб-маркер JSON (JWT), щоб перевірити, чи мав користувач доступ до системи чи ні. Запити перевірялись проміжним програмним забезпеченням і перевіряли, чи має користувач авторизацію чи ні.

Обговорення

На підставі впровадження тестування та результатів, наведених вище, методи тестування TDD та T-BDD показали хороші результати без будь-яких помилок або збоїв для першої та другої фаз. Однак, коли була проведена третя фаза, яка змінювала дані в базі даних, четверта фаза показала помилку для результату тесту TDD. Навпаки, результати випробувань T-BDD все-таки дали задовільні результати.

Крім того, результат також показав, що методи тестування TDD та T-BDD мали свої переваги. Застосовуючи логіку TDD в обох методах тестування, результат тесту покращує відсоток загального покриття тесту в модульному тесті для Vixio, в даному випадку для отримання історії на основі ідентифікатора користувача. Крім того, функція тесту T-BDD здатна підтримувати безперебійну роботу модульного тесту навіть після зміни параметрів, змінюючи вихідні дані всередині бази даних.

Використовуючи T-BDD як комбінацію методів тестування TDD та BDD, цей документ зміг надати докази вдосконалення методу тестування порівняно з використанням лише TDD. Використовуючи метод тестування T-BDD, фази тестування змогли підтримувати загальний відсоток покриття тесту високим, тоді як зміни параметрів ознаки не впливають на результат тестування, поки ціль залишається незмінною.

Висновок

У даній статті було розглянуто метод тестування для серверної системи, поєднавши TDD та BDD у метод тестування T-BDD. Впровадивши простий сценарій для цілей тестування, результат успішно показав, що T-BDD може виконувати тестування програмного забезпечення краще порівняно з тестом

TDD, особливо коли параметри функцій були змінені або розширені. Застосовуючи TDD і T-BDD для внутрішньої системи Vixio, цей документ також зміг показати, що теорія, яка стверджує, що використання методу тестування TDD для отримання високого відсотка охоплення тестом є правильно доведеною. Коли розроблений код, який тестувався, не містив помилок і поведінка не змінювалася, метод тесту працював бездоганно. Крім того, коли середовище було змінено, наприклад, коли фіктивні дані генерувались по-іншому, модульний тест для TDD привів до помилки, яку потрібно було відновити. Тут сценарій BDD у методі тестування T-BDD показав альтернативний метод подолання помилки. Використовуючи метод тестування T-BDD, реалізація тестової функції автоматично переходить з реалізації на поведінку. Для подальших досліджень, щоб забезпечити ефективну роботу T-BDD у будь-яких функціях для тестування внутрішньої системи Vixio (або будь-якого іншого тестування системи), необхідно виконати подальше вдосконалення тесту функції T-BDD. Подальші сценарії тестування з різними функціями також потрібні для забезпечення більш складних умов.

Література:

1. *Vijayasarathy LR, Butler CW. Choice of Software Development Methodologies: Do Organizational, Project, and Team Characteristics Matter? IEEE Software. 2016.*
2. *Kumar N. Software Testing Article - Why is software testing necessary? [Електронний ресурс] – Режим доступу до ресурсу: https://www.utest.com/articles/why-is-software-testing-necessary.*
3. *SM R. What Is Software Testing - Definition, Types, Methods, Approaches. [Електронний ресурс] – Режим доступу до ресурсу: https://www.softwaretestingmaterial.com/software-testing/.*
4. *Sun Y. Unit Testing. In: Practical Application Development with AppRun. Berkeley, CA: Apress Publishing; 2019. p. 247–64.*
5. *CodeUtopia.What's the difference between UnitTesting, TDD and BDD? [Електронний ресурс] – Режим доступу до ресурсу: https://codeutopia.net/blog/2015/03/01/unit-testing-tdd-and-bdd/.*

ШТУЧНИЙ ІНТЕЛЕКТ — «РОЗУМНИЙ БУДИНОК»

Солов'янчик Олександр Андрійович, Овдієнко Станіслав Віталійович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Штучний інтелект (ШІ) — це наука і розробка інтелектуальних машин і особливо інтелектуальних комп'ютерних програм, спрямованих на те, щоб зрозуміти людський інтелект. Але простіше сказати, що це певні команди спрямовані на вирішення певних задач і запрограмовані так, щоб це вирішення було схоже на людське.

Але проблема завжди в тому, що на людину діють певні фактори при вирішенні певних питань, такі як: емоції, настрій, стресова ситуація і т.д. А в штучного інтелекту буде певна послідовність вирішення ситуації тому, що на нього не впливають ніякі фактори, тому між людиною і ШІ буде завжди різниця. Також різниця між людиною і ШІ заключається в тому, що машина, а саме ШІ досить передбачена, а людину передбачити досить важко. «Умний Дом» з наукової точки зору — це свого роду інтелектуальна електропроводка, яка працює на базі керуючої програми. А саме це набір певних команд запрограмованих на роботу всього будинку для полегшення догляду за будинком і полегшення життя самої людини. До розумного будинку входять такі функції, як захист будинку на далекій відстані, також до його функцій входить замовлення продуктів, підтримка температури будинку і повна автоматизація всього будинку з будь якого приладу, на якому існує ОС, а саме такі як iOS, Linux, Android або Windows. Також такий будинок захищений майже від всього наприклад, при вимкненні світла він автоматично включає генератори для підтримки основних можли-востей для підтримки його роботи. Але одна з основних проблем такого будинку це те, що його вартість і обслуговування досить дороге, але найнебезпечніше в таких будинках це те, що він має доступ до всіх ваших фінансових карт, і хоча він захищений від взлому, але можливість його взлому завжди існує. І при взломі злодій зможе за получити доступ до ваших бакських карт з паролями і забрати всі ваші кошти.

Недоліки «Розумного будинку»

Жодна машина не застрахована від збоїв або зависань. Потрібно бути готовим до того, що в будь-який момент знадобиться перенастроювання окремих приладів вручну. Не кожна компанія забезпечить супровід роботи системи. При збої контролера управління сигнал автоматично відправляється не тільки на Ваш смартфон або ноутбук, але і в центральний контрольний центр, розташований в офісі компанії-установника або виробника. Зверніть увагу на надання цієї функції при купівлі Smart House.

Функції смарт-систем

Автоматизація

Майбутнє домашньої автоматизації – це інтелектуальне середовище, здатне за певний час до повернення власника додому встановити потрібну температуру, включивши кондиціонер; відкрити штори або включити музику, почати варити каву і т.д. Звучить неймовірно, але вже сьогодні існують

централізовані системи, здатні виконувати прості побутові завдання, поки господаря немає вдома.

Популярні сучасні смарт-системи:

- Nest;
- HomeKit;
- Wink;
- Z-Wave;
- Zigbee;
- SmartThings;
- Brillo.

В топі поки що тримаються Amazon Alexa, Apple HomeKit і Google Home. Серед розробок можна знайти як більш дорогі, так і бюджетні, наприклад, Orvibo Security Kit.

Технічні гіганти Amazon, Apple і Google роблять ставку на голосових помічників: системи розумного будинку повинні забезпечувати комфорт всім без винятку, особливо допомоги потребують люди з інвалідністю або літні люди, яким важко ходити, управляти побутовими електричними приладами та гаджетами. Тому функція автоматизації вважається пріоритетною.

Енергоефективність

Енергозбереження важливо не тільки для бюджету конкретної сім'ї, а й для планети в цілому. Ефективне витрачання енергетичних ресурсів – актуальна проблема, пов'язана з кліматичними змінами та енергетичною кризою. Витрата енергії побутовою технікою у той час, поки вона не використовується (наприклад, годинники на мікрохвильовій печі або на панелі духової шафи працюють навіть тоді, коли техніка нічого не розігріває і не пече) – це так зване "фантомне навантаження". Домашня автоматизація, виконувана AI, знижує споживання енергії і викид вуглекислого газу за рахунок керування "розумними" термостатами, роз'ємами і давачами освітлення.

Безпека

Застосування штучного інтелекту і нейронних мереж глибокого навчання активно відбувається у соціальних мережах. Наприклад, Facebook використовує технологію розпізнавання осіб, її точність становить 97%. "Розумні" системи безпеки на підприємствах оснащені датчиками руху та інтелектуальними камерами: вони вміють розпізнавати загрозу злому і навіть можуть викликати екстрені служби.

Приклад рішення, що забезпечує інтернет-безпеку в будинку: система Bitdefender BOX від компанії Bitdefender. Рішення пропонує захист для розумних телевізорів, приставок,

комп'ютерів, у тому числі і дитячих; запобігає інтернет-атакам, хакінгу і виявляє загрози у системі безпеки.

Створення дружнього середовища

До завдань системи розумного будинку входить не тільки забезпечення безпеки або автоматизація рутинних процесів. Створити комфортне і дружнє середовище, в якому людина не буде відчувати себе гостем – ось один з пріоритетних напрямків діяльності смарт-системи. Одна з таких систем це Josh.ai, програма домашньої автоматизації з голосовим управлінням. Так само як всім відома Siri або Google Now, Josh створений для розпізнавання голосових команд на природній мові. Це означає, що програма сприймає вітання, запитання, інструкції та багато іншого. До системи можна підключити будь-який розумний пристрій, наприклад, кондиціонер або систему освітлення. Основний бонус використання такого рішення – просте управління цілим будинком з будь-якої його точки. Josh і подібні до нього додатки формують комфортне, дружнє середовище в просторі навколо користувача.

Чого очікувати у найближчі роки?

Згідно з дослідженням ринку штучного інтелекту як послуги (AIaaS), проведеного компанією Technavio, обсяг інвестицій в ШІ в 2019 році збільшиться на 47%. У звіті аналітики підкреслюють зростання попиту на "розумні" будинки і розвиток розумних міст (як одну з основних світових тенденцій). Концепція розумних будинків буде ставати все більш популярною, основна увага приділятимется електронним пристроям і автоматизації їх роботи.

У той же час, глобальний ринок штучного інтелекту як послуги (AIaaS) почне відчувати нестачу кваліфікованої робочої сили. На виробництвах затребуваними залишаться технології обробки природної мови і взаємодія людини з роботизованими системами.

Література:

1. *sdamzavas.net - Поняття штучного інтелекту*
2. *smarthouse Умный Дом SmartHouse - Что такое Умный Дом*

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Суханов Владислав Романович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Розвиток IT-технологій допомагає підвищити ефективність суспільного виробництва в усіх сферах. Можливість пошуку, управління, обробки й обміну інформацією розкриває нові горизонти, дозволяє максимально автоматизувати

будь-які промислові процеси, підвищити показники праці та полегшити управління бізнесом.

Сучасні інформаційні технології повинні бути максимально доступними споживачам, щоб вони могли без витрат часу й сил проводити різноманітні операції.

Організація швидкого доступу до всіх інформаційних ресурсів, необхідних для роботи, гарантує підвищення економічних показників підприємств будь-якого сектору й покращення умов праці для персоналу.

За типами оброблюваної інформації ІТ-технології можна умовно розділити на такі види*:*

Дані (алгоритмічні мови, табличні процесори);

Текст (текстові процесори та гіпертекст);

Графіка (графічні процесори);

Знання (експертні системи);

Об’єкти сучасного світу (мультимедіа).

Більшість сучасних технологій дозволяє використовувати одразу декілька видів обробки інформації. Наприклад, в текстових редакторах є можливість створювати таблиці розрахунку даних, в таблицях можна використовувати графіки і т.ін.

Але кожний метод обробки орієнтований для проведення операцій із визначеним видом інформації, тому модифікація елементів з різних сфер дозволяє створювати нові технології, якими на даний момент користуються вузькопрофільні підприємства, заводи, фабрики й компанії.

Література:

1. *https://tsn.ua/ru/nauka_it/osnovatel-tesla-planiruet-sozdat-kosmicheskiy-internet-i-svyazat-zemlyu-s-marsom-406132.html*

2. *https://www.it.ua/knowledge-base/technology-innovation/dopolnennaja-realnost-ar*

3. *http://thefuture.news/page1837780.html*

ЗНАЧЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЖИТТІ ЛЮДИНИ

Трощій Анастасія Олександрівна

Харківський національний економічний університет ім. Семена Кузнеця

м. Харків

В даний час, практично всі люди володіють тією чи іншою інформацією, яку людина отримує з різних джерел. Сама по собі інформація - це сукупність відомостей про навколишній світ, про всілякі процеси, що трапляються у ньому, які можуть бути сприйняті інформаційними системами. Процеси перетворення інформації пов'язані з інформаційними технологіями.

Інформаційні технології - це все, що пов'язано з обробкою, збереженням і передачею даних. І сьогодні вони оточують нас у всіх сферах життя. Хочемо ми того чи ні, вони стали частиною сучасного суспільства.

Найбільш значуща подія в цій сфері є створення глобальної мережі «Інтернет». Це унікальний винахід здатний зробити життя людини краще. По-перше, це можливість швидко знайти потрібну інформацію, не виходячи з дому, так як раніше це займало багато часу. По-друге, це все, що пов'язано з соціумом, а саме, спілкування. У сучасному світі зовсім немає проблем спілкування з людьми, які знаходяться від тебе в тисячах кілометрах. Крім усього перерахованого вище, це велика можливість урізноманітнити своє дозвілля. Тобто, Інтернет може надати всю ту інформацію, яка для людини буде важлива.

Можу припустити, що інформації стає все більше, і деяка вже не несе в собі те смислове навантаження, яке було раніше, вона стає неактуальною, але продовжує перебувати в Інтернеті. І за допомогою інформаційних технологій, треба спробувати впровадити фільтрацію.

Так як у нас зараз все перейшло в електронний формат, потрібна нам інформація зберігається у кожної людини на електронних носіях, тому є потреба в захисті персональних даних. Під цим мається на увазі захист не тільки особистої інформації, а захист більш глобального масштабу. Обсяг конфіденційної інформації комерційних компаній і держструктур надзвичайно широкий. Це комерційні таємниці, ноу-хау, особисті дані співробітників, клієнтські бази і так далі. Такі відомості дуже цінні для шахраїв і потрапляння такої інформації в руки конкурентів або кіберзлочинців може спричинити для організації та її клієнтів далекосяжні юридичні наслідки, непоправні фінансові та репутаційні втрати.

В сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексним системним захистом інформації, який повинен бути: безперервним, плановим, цілеспрямованим, конкретним, активним, надійним і ін. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і критичних ситуаціях.

Підводячи підсумок, можна сказати, що інформаційні технології сьогодні відіграють винятково важливу роль у забезпеченні інформаційної взаємодії між людьми, а також в системах підготовки і поширення масової інформації.

Література:

1. Бирюков А. А. Информационная безопасность: защита и нападение / А. А. Бирюков., 2016. – 436 с.

2. Математика и информатика : учебник и практикум для среднего профессионального образования / Т. М. Беляева [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 402 с.

3. Інформаційна безпека now [Електронний ресурс] – Режим доступу до ресурсу: https://www.prostir.ua/?library=informatsijna-bezpeka-now-yakyh-elementiv-ne-vystachaje.

ОНЛАЙН ІТ-ОСВІТА: МОЖЛИВОСТІ, РЕСУРСИ, ТЕХНОЛОГІЇ

Файчук Ліна Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Статтю присвячено дослідженню особливостей онлайн ІТ-освіти. Проаналізовано поширені на сьогодні середовища для вивчення основ програмування, з'ясовано основні характеристики, методи й механізми навчання. Проведений аналіз освітніх ресурсів демонструє різноманіття програм, напрямів, умов. Відзначено перспективність і надзвичайну актуальність для онлайн ІТ-освіти впровадження технологій гейміфікації в навчальний процес. Доведено, що онлайн ІТ-освіта – мобільний та дієвий спосіб отримання нових знань, що потребує високої мотивації та самоконтролю.

В умовах стрімкого розвитку технологій, динамічних змін на ринку праці необхідність здобувати додаткові кваліфікації і знання, удосконалювати та покращувати вже набуті навички або навіть кардинально змінити спеціальність є надзвичайно актуальними. Головні вимоги, які висуває потенційний споживач, – навчання має бути доступним, гнучким та мобільним, не повинно займати багато часу, але давати максимум результату.

У зв'язку з цим онлайн-освіта набирає все більших обертів. До того ж Covid-19 вніс суттєві корективи в більшість сфер життєдіяльності людини, в тому числі навчальну: школи та вищі навчальні заклади були змушені перейти в онлайн-формат, кардинально змінивши стратегії викладання. Крім цього, освіта та наука є сферами, у яких запроваджується найбільше програм із гейміфікованими елементами та створено велику кількість додатків і платформ.

Поширеними на сьогодні є середовища для вивчення основ програмування, мобільного вивчення різноманітних курсів і дисциплін в ігровій формі. Для подальшого дослідження наявних освітніх ресурсів з'ясуємо вагомі чинники. Так, онлайн-освіта буває платною та безкоштовною, також розрізняємо онлайн-навчання індивідуальне (студент вивчає матеріал без взаємодії з викладачем та групою) та синхронне (навчання групи

студентів, спілкування з викладачем через інтернет). Відзначимо, що кожний з видів навчання має свої переваги та недоліки. Зокрема, плюсами індивідуального навчання вважаємо можливість отримувати знання в зручному форматі (переносити лекції, повторно їх переглядати), водночас такий підхід може спричинити втрату системності занять. Наявність і відсутність групи й викладача також можна оцінювати по-різному. З одного боку, – це елемент соціалізації і можливість відразу отримувати відповіді на питання, з іншого, – виклик і прагнення заглиблюватися і з'ясовувати незрозуміле самостійно. За таких обставин результат великою мірою залежить від мотивації студента.

Важливим, на нашу думку, є насамперед аналіз безкоштовних online-ресурсів для вивчення програмування [3, с. 52].

Найбільшим проектом безкоштовної освіти в Україні є платформа Prometheus, місія якої – зробити найкращі курси від провідних викладачів, університетів та організацій світу доступними для всіх [https://prometheus.org.ua/about-us/]. Платформа пропонує низку безкоштовних курсів різного рівня та спрямування, зокрема, курс «Алгоритми і проекти Scratch» – перше знайомство з програмуванням, курс «Основи програмування» – можливість навчитись створювати нескладні алгоритми за допомогою мови Python; курс «Розробка та аналіз алгоритмів» – більш фундаментально про комп'ютерні алгоритми; курс «Основи тестування програмного забезпечення» – базові знання, необхідні тестувальнику програмного забезпечення; курс «Основи Web UI розробки» – базові знання з веб-розробки; курс «Основи програмування CS50» – легендарний курс Гарвардського університету, тощо.

Окремий блок платформи – Prometheus+ є платним. Сюди входять курси, що створюються зірковими викладачами та компаніями. Таким чином, працює механізм подальшого розвитку платформи і створення нових безкоштовних курсів. По кожному курсу Prometheus+ потенційний споживач може отримати вичерпну інформацію про всі важливі деталі та особливості.

Так, курс «Основи Python» допоможе зробити новий крок до професії data scientist, веброзробника або розробника вебзастосунків. Програма курсу включає 50+відеолекцій, практичні завдання в розробницькому середовищі, а також тести на закріплення знань, 13 онлайн-зустрічей з викладачем по 2 години щотижня та 2 вебінари, Чат-підтримку в Slack

викладачем та кураторами курсу для розв'язання усіх питань, 2 міні проєкти (розробка гри та магазину за допомогою матеріалів курсу).

Відзначимо інший безкоштовний ресурс edX (англійською мовою) із більш профільним курсами: курс «Android Development» – створення свого власного додатка для мобільного; курс «Cloud Computing» – вивчення хмарних технологій; курс «R Programming Courses» – мова програмування для статистичної обробки даних та роботи з графікою; курс «Robotics» – створення роботів та машинне навчання.

Зокрема, платформа edX пропонує різні курси вивчення основ Python: Основи Python для науки про дані від IBM; Обчислення в Python I: фундаментальне та процедурне програмування від GTx; Машинне навчання за допомогою Python: практичний вступ від IBM; Використання Python для дослідження від ГарвардX. Так, тривалість курсу Основи Python для науки про дані від IBM складає 5 тижнів, займатиме 2-5 годин на тиждень, є безкоштовним (оплачується лише сертифікат), англомовним, рівень – вступний (початковий). Детально також на сайті платформи розписано програму курсу за модулями з конкретизацією тем та кінцевих знань і навичок [https://www.edx.org/course/subject/computer-science].

Окремо виділяємо групу ресурсів, які пропонують курси безкоштовно, але оплата за навчання здійснюватиметься після працевлаштування.

Так, Mate academy – онлайн академія IT професій, яка пропонує 100% онлайн навчання (20% теорії, 80% практики), працевлаштувала більше 800 випускників, додаткова опція – безкоштовна англійська. Академія передбачає два формати навчання: повного дня (є безкоштовним до працевлаштування, тривалістю 4 місяці, з понеділка по п’ятницю з 09:00-18:00; ціна – 17% з кожної заробітної плати протягом 2-х років незалежно від міста працевлаштування) та «Вечірнє» навчання (14 днів безкоштовно, далі оплата помісячно, графік навчання – вільний, тривалість 300 годин; ціна за 1 календарний місяць від 2 895 грн.) [https://mate.academy/]. Стратегія компанії, на нашу думку, містить певні маніпуляційні технології, гарантії та бонуси, які варто уважно враховувати. Для того, щоб потрапити на курси за певним напрямком, потрібно пройти 3 етапи. Перший етап: на сайті mate.academy обрати курс та заповнити форму з контактними даними (у ній будуть також вказані вимоги до знань та навичок, короткий опис технологій, які буде розглянуто протягом курсу). Другий етап: виконання тестового завдання,

що надходить на пошту. Третій етап: за позитивних результатів тесту відбувається співбесіда з координатором академії (в тому числі, перевірка рівня англійської мови). Після отримання остаточної позитивної відповіді здійснюється безпосереднє підписання договору.

Варто зауважити, що на сайті Mate academy програми окремих курсів (зокрема, Java Core) недостатньо деталізовані. Це ж стосується і поданого плану навчання на тиждень, який містить узагальнені неконкретні категорії: алгоритмічні задачі, заняття, практична робота, розбір [https://mate.academy/courses/java].

На сьогодні фахівці ІТ-освіти намагаються знайти максимально цікаві, дієві та комфортні підходи до процесу навчання. Серед них надзвичайно ефективним, на нашу думку, є залучення інструментів гейміфікації. За визначенням С. Переяславської, О. Смагіної «Гейміфікація в освіті – це процес поширення гри на різні її сфери, який дозволяє розглядати гру і як метод навчання і виховання, і як форму виховної роботи, і як засіб організації цілісного освітнього процесу [2, с. 251].

До основних компонентів гейміфікованого процесу навчання відносять: завдання, які виконують користувачі, прогрес у визначенні цілей; бали, які накопичуються в результаті виконання завдань; рівні, які долають користувачі; значки, що слугують нагородою за завершення дій; ранжування користувачів відповідно до їхніх досягнень.

До ігрових елементів, що формують механіку процесу гейміфікації, належать: виклик (мета для досягнення); завдання, тести; співробітництво (виконання роботи над помилками, взаємодопомога при вирішенні завдань); зворотний зв'язок (інформація про успіхи гравця); накопичення ресурсів (показників знань); винагороди (бонусні бали, нагороди, бейджики, віртуальна валюта); стан перемоги (шкала досягнень, сумарний показник балів, поточний показник знань з урахуванням бонусів, підсумкова оцінка, рейтинг) [2, с. 252].

Так, онлайн лабораторія програмування Programmr.com пропонує багато курсів PHP, Java, C++, Python та інші. Платформа робить найкращі у світі онлайн-симулятори кодування. У Programmr можна кодувати, компілювати та запускати проекти прямо в браузері майже будь-якою мовою. За допомогою нового модуля автоматичного викладання є можливість оцінити свої вміння будь-якою популярною мовою програмування, пройшовши практичні вправи. Таким чином, основний акцент робиться на перевірці вже здобутих знань за допомогою інтерактивних вправ. Також ресурс пропонує

конкурси із програмування із грошовими преміями [http://www.programmr.com/about_us].

Платформа CheckiO виділяється тим, що призначена насамперед для практики та вдосконалення навичок; має не лише значну кількість цікавих завдань з кодування та різноманітних інструментів для розв'язування головоломок, а наповнена цікавими та унікальними рішеннями. Відповідно, вчителі в усьому світі використовують CheckiO як додатковий інструмент, аби студенти могли відпрацьовувати навички під час вивчення нового матеріалу. Ресурс надає вчителям таблицю, де можна побачити список учнів, інформацію про те, коли останній раз кожен з них був активним, та місії, які вони реалізували чи намагалися реалізувати. Прогрес класу дає чітке уявлення про те, як клас працює на CheckiO і які завдання виявились найскладнішими для учнів [https://checkio.org/].

Щоразу, коли хтось із студентів виконує місію, зберігається журнал того, як він прийшов до цього результату, можна побачити етапи, використані підходи, можливі труднощі. Це об'єктивно ефективний спосіб контролювати свій клас, зрозуміти, як студенти використовують матеріал на практиці, відповідають на завдання та знаходять рішення.

Абсолютно новою концепцією, яка навчає програмуванню, розважаючись, є CeeBot. Це низка програмних продуктів, адаптованих до різного віку та потреб. Зокрема, CeeBot4 (15-99 років) можна використовувати як гру для вивчення програмування або для викладання програмування в середній, вищій школі та університеті. За допомогою мови програмування програмуються роботи, які виконуватимуть різні завдання, починаючи від пошуку виходу з лабіринту через автоперегони до гри у футбол. Кожна вправа починається з точних вказівок, часто доповнених ілюстрацією, пояснюються цілі та основні принципи програмування. Кожна програма CeeBot має понад 50 прогесивних вправ [http://www.ceebot.org/].

Отже, онлайн ІТ-освіта – мобільний та дієвий спосіб отримання нових знань, що потребує мотивації та самоконтролю. Проведений аналіз освітніх ресурсів демонструє різноманіття програм, напрямів, умов. Перспективним і надзвичайно цікавим для онлайн ІТ-освіти є впровадження технології гейміфікації в навчальний процес.

Література:

1. Ковалюк Т., Єфіменко О. Про розвиток ІТ-освіти України. http://ena.lp.edu.ua:8080/bitstream/ntb/12575/1/049_Kovaljuk_293_297_719.pdf

2. Переяславська С. Гейміфікація як сучасний напрям вітчизняної освіти / С. Переяславська, О. Смагіна // Відкрите освітнє е-середовище сучасного університету.

2019. Вип. спецвип.. С. 250-260. Режим доступу: http://nbuv.gov.ua/UJRN/oeeemu_2019_spetsvip._26

3. Шаров, С. В., Печерський, Р. В. (2018). Аналіз відкритих онлайн курсів для вивчення програмування. Проблеми та інновації в природничо-математичній, технологічній і професійній освіті: зб. матеріалів VI-ї Міжнар. наук.-практ. онлайн-інтернет конф. м. Кропивницький, 19-20 квітня 2018 р. С. 52-53.

ТЕХНОЛОГІЯ БЕЗДРОТОВОЇ ЗАРЯДКИ MI AIR CHARGE

Філімець Ростіслав Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Ринок IT стрімко розвивається. Кожного року на полицях магазинів техніки з'являється безліч цікавих новинок. В той же час, існує мало компаній, які по-справжньому задають тренди у світі технологій, а не користуються напрацюваннями минулих років. Китайська корпорація Xiaomi - одна з таких. Її смартфон Mi Mix мав практично безрамковий дисплей. До того ж, компанія вважається піонером в області технологій заряджання. Вона представила бездротову зарядку потужністю 80 Вт. Але сьогодні бренд вийшов на новий рівень, оголосивши про Mi Air Charge. Це - технологія, що дозволяє заряджати кілька пристроїв одночасно без використання дротів чи інших звичних аксесуарів.

Технологія бездротової зарядки Xiaomi під назвою Mi Air Charge була оголошена зовсім нещодавно. Як стверджується, вона дозволяє заряджати декілька пристроїв одночасно без підключення будь-яких кабелів або розміщення пристрою на підставці для бездротової зарядки.

Ізольований зарядний блок Xiaomi власної розробки має п'ять вбудованих антен, які можуть максимально точно визначати місце розташування смартфона. Масив управління фазою, що складається зі 144 антен, передає хвилі міліметрового діапазону безпосередньо на телефон за допомогою формування променю.

Така зарядка не має зовсім нічого спільного зі стандартом Qi. Смартфони повинні бути оснащені 14 мініатюрними антенами для перетворення сигналу міліметрового діапазону, що випромінюється зарядним пристроєм. Сигнал таким чином перетворюється в електричну енергію через схему випрямляча.

У поточному стані технологія віддаленої зарядки Xiaomi може одночасно заряджати декілька пристроїв струмом 5 Вт в радіусі «кількох метрів». Xiaomi стверджує, що фізичні об'єкти ні в якому разі не знижують ефективності зарядки.

Глава мобільного підрозділу компанії Xiaomi - Адам Цзен Сюечжун - рішуче запевняє, що за допомогою інноваційної

технології Mi Air Charge Technology в найближчому майбутньому планується заряджати ще й інші пристрої. Наприклад такі, як розумні годинники та фітнес-трекери.

Література:
1.https://www.gsmarena.com/xiaomi_introduces_mi_air_charge_wireless_charging_from_across_the_room-news-47461.php
2.https://www.gizmochina.com/2021/01/29/xiaomis-mi-air-charge-technology-brings-a-true-wire-free-charging-experience/

ОПТИМІЗАЦІЯ СЕРВЕРНИХ ОС ДЛЯ ОСОБИСТОГО ЗБЕРІГАННЯ ДАНИХ

Цвик Олександр Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м.Київ

Мета: *формування самостійної підбору обладнання для домашнього серверу NAS. Підбір та обґрунтування серверних операційних систем та програмного забезпечення , що допоможе збільшити ефективність використання NAS. Оптимізація операційних систем ті налаштування для використання на домашньому сервері. Пошук найкращої системи під NAS-домашнього сервера та програмного забезпечення, для кращого доступу під системи та його резервування.*

На 2021 рік технології зі зберігання даних просунулися далеко вперед. Є різні способи зберігати інформацію: на знімному носії, всередині комп'ютера або на сервері. Більшість малих і середніх компаній використовують особисті сервера для зберігання робочих даних співробітників, а великі компанії воліють ЦОД.

Для цивільних людей так само надають хмарне зберігання:

- Dropbox.
- «Google Диск»
- Apple iCloud.
- Huawei Cloud.
- Microsoft OneDrive і т.д.

Хмарні технології - це служба, яка дозволяє зберігати дані Шляхом їх передачі по інтернету або Іншої мережі в систему зберігання, что обслуговується третьою стороною

Хмарне зберігання почало набирати популярність після 2010 року. Спершу компанії почали цікавитися таким видом зберігання даних, і ближче до 2015 року вже і половина населення планети використало Google Drive і iCloud.

Переваги зберігання даних було вираженого в його доступності та сумісності з декількома людьми або компаніями:

• Доступ до даних з будь-якого комп'ютера, що має покдлючення до інтернету

• Спільна робота з даними для різних людей \ компаній

• Збереження даних при критичному збої

• Покупець місця в хмарі не переплачувати за обслуговування і модернізацію серверів або ЦОД

• Резервування та збереження даних в хмарі.

Так само є проблеми в хмарному зберігання, які заважає багатьом користуватися: безпека і загальна продуктивність.

Вже починаючи з 2018 року люди, пов'язані з IT індустрією, почали замислюватися про використання домашнього сервера з хмарою зберігання особистих даних.

Багато виробників жорстких дисків або серверного обладнання почали пропонувати суспільству малий док-станцій, в які можна було помістити від 2-х жорстких дисків і управляти ними з робочого комп'ютера. Таки станції не займають багато місця, вони компактні і легко керовані. Їх залишається тільки підключити до ДБЖ (джерела безперебійного живлення) для додаткової безпеки даних.

Так само такі док-станції спокійно можна підключати до малих серверів, які більшість використовують вдома. Так можна надати більше можливостей у використання хмарного зберігання.

Для оптимізації користування домашнім сервером, використовую серверного ОС. Є три компанії. Які Головні в сфере ОС для серверів. Смороду починаєм розробка однаково й йшли пліч-о-пліч 30 років и це: Microsoft Windows, UNIX, та UNIX-подібні системи.

FreeBSD- операційна система для серверів випущена в 1993 і по праву вважається найстарішою з усіх. На 2021 рік існує більше 10-х версій цієї ОС. FreeBSD була створена на основне UNIX-ядра з відкритим кодом, через що вона походу на Linux[2,с. 12-14]

Протягом багатьох років ця система вважалася однією з найстабільніших. Після того як BSD отримав відкритий вихідний код, з'явилися і інші похідні цієї ОС - OpenBSD, NetBSD, DragonFly BSD. І найпростіша система з них - якраз Free BSD, яка розрахована на звичайних користувачів.

Так як ця система мати відритий вихідний код, і досить стара, вона має проблеми з підтримкою. Більшість проблем або багів залишається невирішеними

Windows server - популярна ОС для малих і середніх компаній. Система дозволяє використовувати всю продуктивність сервера. Так само для Windows Server випускають багато додатків і програм, які доступні як безкоштовно, так і платно. В основному операційну систему

встановлюють для файлових серверів, так як перевага в інструментах і програм для резервування і бекапов системи.

Недоліками системи є велика кількість шкідливого ПЗ. Вони можуть бути як і в піратському ПЗ так і в безкоштовному ПО. Windows Server має тільки ліцензовані копії, тому вони не підходять до серверів, кількість яких не перевищує 3-х штук.

Кращим дистрибутивом для серверів комерційних і особистих вважається Linux і Linux-подібні системи

Стабільність і надійність забезпечує Debian 9, для якого випущено 51687 пакетів. Більшість вважають її консервативної, однак Debian швидше, ця система надійна, стабільна і довговічна. Ця операційна система була випущена в 00-х, але розробники продовжують підтримувати її і в 2021-му.

Кілька особливостей актуальною ОС Дебіан для серверів:

- Підтримка архітектури: i386, amd64, armel, armhf, mips, mipsel, ppc64el, s390x;
- Файли з метаданими завантажуються по хешу вмісту;
- Застосування APT A SRV в DNS з метою визначення бекенд загрузкі.В цієї операційки є всі необхідні підтримувані технології, включаючи PHP 7.0, Python 3.5, JAVA 8, ядро Linux 4.9, LibreOffice 5.2 і інше.

Debian однозначно підходить для використання на файлових серверах, веб-вузлах і терміналах.

Rad Hat - популярна операційна система на основі Linux, яка переважно використовується в корпоративних цілях. Саме цю систему часто використовують при розгортанні глобальних інформаційних проектів, в телекомунікаційних компаніях, фінансових установах і навіть на світових фондових біржах.[4, с. 20]

ОС платна. Її актуально використовувати не для одиночних серверів, а для цілих корпоративних дата-центрів і роботи цілих веб-вузлів з високою продуктивністю

CentOS - це безкоштовна версія дистрибутива Linux, яка дуже схожа на Red Hat, але для приватного використання. Перевагою є не тільки відсутність плати за користування, а й доступ до менеджера пакетів yum, а також підтримка багатьох панелей управління хостингом. Правда, через безкоштовного розповсюдження багато технічних питань доведеться вирішувати самому (ну або IT-інженеру компанії), так як служба підтримки працює слабо. Але багато користувачів діляться на тематичному форумі про вирішенні виникаючих у них багів або проблем (в цілому, ОС працює стабільно без збоїв).

Ubuntu - проста операційна система на базі Linux, яка використовується для серверів з невеликим навантаженням.

Налаштування цієї ОС проста, тому з нею впорається навіть користувач з мінімальним досвідом. По інтерфейсу і підтримуваним утилітам ця операційна система чимось схожа на Debian.

Уніфікованого відповіді на це питання немає. Під різні завдання і категорію користувачів підходять ті чи інші версії операційних систем. Наприклад, CentOS і Free BSD вважаються вже застарілими варіантом, а все більше серверів зустрічаються на Windows Server або Linux (Ubuntu або Debian). Red Hat підходить для великих дата-центрів - цю систему рідко зустріти на серверах малих і середніх компаній. Windows Server - більш універсальний варіант з широким вибором програмного забезпечення. Але новачки навряд чи зможуть швидко розібратися з мануалом цієї системи. Для простих завдань вибирають Ubuntu або Debian, які відрізняються актуальним софтом і зручним інтерфейсом.

Можна виділити кілька основних факторів, з урахуванням яких і вибирають операційні системи для серверів:

Безпека - під операційну систему створено дуже мало вірусів (це відноситься до Linux, але аж ніяк не до Windows Server);

Надійність - в даному критерії теж виграє Linux, так як він може працювати навіть без деяких драйверів або без графічного процесора, на відміну від Windows Server);

Вартість - деякі ОС поширюються безкоштовно і підходять більше для простих завдань, а інші тільки по ліцензії для корпоративного застосування;

Віддалене адміністрування - в Linux є вбудовані команди для віддаленого управління, а в Windows Servers доступно тільки локальне адміністрування.

Так для домашнього сервера підходять CentOS або Ubuntu.

Але не тільки ОС допоможе нам зберігати дані на сервері, а й спеціальні додатки. Додатків для домашнього користування не багато, як для компаній.

FolderSync забезпечує просту синхронізацію файлів в хмарним сховище і в локальних папках на SD-картах пристрою. Він підтримує широкий спектр різних хмарних провайдерів і файлових протоколів і постійно додається безліч нових платформ. Доступ до кореневого файлу підтримується на рутірованних пристроях.

В операційній системі DiskStation Manager є вбудований репозиторій пакетів Package Center з безкоштовними сервісами, які підтримує NAS. Установка відбувається так само, як в будь-

якому магазині додатків: вибрав сервіс, натиснув кнопку завантаження, встановив.

DiskStation Manager підтримує роботу з декількома користувачами. Кожному можна обмежити швидкість підключення, доступ до конкретних папок і сервісів, визначити квоти за обсягом трафіку. Усередині сервісів доступні докладні настройки в залежності від їх функцій: наприклад, обмеження доступу до конкретних файлів знадобиться для домашнього використання (у кожного члена сім'ї є своя папка) і для спільної роботи з файлами.

Е две операційних системи, Які підходять під різні типи завдань. CentOS та Ubuntu основні системи під різні типи та сфера использование.

Сервера, на якіх будут Встановлені ОС, ма ють різну апаратної часть, яка дозволяє без проблем та Найкраще використовуват всю систему. Праця CentOS Залежить від правильно налаштованої апаратної часті и також від ресурсов, что вона має. Ubuntu вікорістовує малу часть ресурсов но має буті налаштовано сама ОС.

Ubuntu Підходить для дата-центрів від малих до великих. Альо использование может буті й в малих системах. CentOS Використовують в основном Великі компании, тому что така операційна система травні надійну та стабільну працю.

Враховуючі вищє наведені аргументи, Найкращий Вибори буде Ubuntu server. Ubuntu має велику предпочтение у віборі между іншімі системами.

Безкоштовна - система, якові можливо скачать з офіційного сайту, потребує навчання персоналу, если Системні адміністратори НЕ ма ють досвіду налаштування системи. Також основні програми для использование на системе є безкоштовна.

Стабільна - вікорістовуючі якові є можлівість працювати более трех місяців без перезавантаження та віключення. Буває система может працювати в течение року без перебоїв й помилок.

Швидка - при вікорістанні малої кількості ресурсов, система має змогу швидко опрацьовуваті дані та інформацію. Також Такі системи є надійнімі в вікорістанні на серверах.

Багатофункціональність - нараховує велику Кількість особливо функцій для продуктівної праці та повного навантажження системи для кращої праці. Такі Функції підходять для різноманітніх завдань, як і управління персоналом та и налаштування та Поліпшення праці в дата-центрі.

Безпека - в систему встановлен служба захисту від вторгнення вірусів та зловмісників з глобальної мережі. Такий захист допомагає НЕ встановлюваті Допоміжні Додатки та антівірусі в систему (для полного захисту системи нужно встановлюваті допоміжне обладнання).

Унікальність - система має Унікальні решение задач. Много ролей та службових сервісів, что підходять під різноманітні Розширення системи.

При віборі системи, треба прійматі до уваги всі Преимущества система та Недоліки. CentOS має перевага у в стабільності системи, но вона Вже НЕ буде оновлюватіся, после того, як ее викуп RedHat компанія. Ubuntu server є багатофункціональною системою, но Кожне оновлення додає много багів на недоліків в відкрітому коді.

Література:

1. https://habr.com/ru/post/430970/

2. Декет В.М. FreeBSD 9. Корпоративный Интернет-сервер. –К.: ФЛП Декет В.М., 2013 – 176 с.

3. Data Center Handbook V5.0 02/2014 Reichle & De-Massari AG R&M URL:http://www.synergia.ua/images/content/Tatiana.Golovaschenko/RM_Data_Center-Handbook_V5.pdf

4. «Открытые системы. СУБД» выпуск №06, 2006 URL : https://www.osp.ru/os/2006/06/2700569/

ЕКОНОМІЧНИЙ ТА СОЦІАЛЬНИЙ ВПЛИВ ІНТЕРНЕТУ РЕЧЕЙ

Чіганов Богдан Олександрович

Державний університет телекомунікацій

Навчально-науковий інститут Інформаційних технологій

м. Київ

Зазначено технологічні зміни, характерні для сьогодення та ті, що окреслюють перехід у нову технологічну революцію, яка змінює спосіб суспільної праці й людського буденного життя, позбавляє суспільство необхідності самостійно виконувати певні завдання, роботу, обслуговувати інших осіб. Відзначено, що сьогодні поява таких явищ, як: фізична присутність технологічних інновацій в інтелектуальних продуктах, послугах, виробництві товарів призводить до поєднання цифрових, фізичних, біологічних технологій, до утворення кібер-фізичних систем. Відзначено, що сьогодні поява таких явищ, як: фізична присутність технологічних інновацій в інтелектуальних продуктах, послугах, виробництві товарів призводить до поєднання цифрових, фізичних, біологічних технологій, до утворення кібер-фізичних систем. Вищеозначене свідчить про те, що теперішнє суспільство, світ і технології мають поєднуватися у тріаду: інтернет – кіберфізичні речі - інтернет речей. У зв'язку із цим, проаналізовано динаміку кількості підключених осіб та пристроїв до світової мережі інтернет та, яка кількість цих пристроїв припадає на душу населення; виявлено, що за аналізований період з появою смартфонів та планшетних комп'ютерів відбулося стрімке зростання підключень пристроїв до глобальної мережі.

На основі аналізу різних статей була складена авторська класифікація ринку Інтернету речей, в основі якої в якості критерію обраний суб'єкт ринку Інтернету речей - споживачі (споживчий сегмент Інтернету речей), держава (державний сегмент Інтернету речей).

В переліку найкращих сфер застосування технологій IoT сфера охорони здоров'я займає одну з найважливіших ланок. Інтернет речей впливає безпосередньо на життя людей та показує важливість медицини як сфери діяльності в сучасному суспільстві.

Саме завдяки IoT лікарі можуть допомагати людям через інтернет. За останні роки техніка пішла далі й уже медичні дрони готові прилетіти вам на допомогу з потрібними ліками. В генетиці завдяки IoT робляться цілі відкриття! IoT дозволяє знайти підхід до кожного пацієнта окремо, проаналізувати стан його здоров'я та прорахувати індивідуальний метод лікування. Розробка інтернет-застосунків на цей час все ще має деякі труднощі, особливо якщо брати до уваги інтернет речей і традиційну медицину. Але IoT у сфері охорони здоров'я розвивається дуже швидко.

Щоб детально розповісти про можливості IoT-пристроїв в будинку, буде потрібно написати окрему статтю, бо їх доволі багато. Наприклад, існують розумні термостати, кондиціонери, колонки, навіть годівниці для тварин та інші повсякденні пристрої, які виконують звичайні домашні функції. Це одна з найпопулярніших та перспективних сфер використання інтернету речей.

До IoT-технологій міста відносять розумне паркування, карти шуму, розумне освітлення та дороги. Хоча зараз ця сукупність пристроїв перебуває на стадії планування та розробки, але вони мають доволі далекоглядні перспективи. За допомогою IoT-технологій можна збільшити безпеку на міських дорогах, краще контролювати рух міського транспорту і забруднення великих індустріальних населених пунктів.

Висновок

Слід зазначити, що велика частина населення не помічає, як технології Інтернету речей стають частиною їх повсякденного життя. Вже зараз майже кожний може відчути на собі ефективність та швидкість методів лікування з застосуванням технологій Інтернету речей. Також набуваючи нові апартаменти, споживачі часто отримують нове житло з вбудованими рішеннями Інтернету речей, спрямованими на економію споживаної електроенергії і води. Саме тому для вирішення виникаючих соціальних проблем необхідно реалізовувати

програми з підвищення обізнаності великих груп людей, щодо застосування технологій Інтернету речей.

Література:

1. Кілька найпопулярніших сфер використання інтернету речей: https://lpnu.ua/news/kilka-naipopuliarnishykh-sfer-vykorystannia-internetu-rechei

2. ІНТЕРНЕТ РЕЧЕЙ ЯК СКЛАДОВА ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ: http://www.economy.nayka.com.ua/?op=1&z=5315

АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ ТА ЗАСТОСУВАННЯ СИСТЕМ КОМП'ЮТЕРНОГО ЗОРУ

Шевченко В.І.
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Системи комп'ютерного зору є одним з найбільш затребуваних напрямів в сучасному світі IT. Комп'ютерний зір (Computer Vision, CV), в тому числі машинний зір (Machine Vision, MV) - це автоматична фіксація і обробка зображень, як нерухомих, так і рухомих об'єктів за допомогою комп'ютерних засобів. В останні роки CV стало активно використовуватися в промисловості, в т.ч. в таких галузях, як автомобілебудування, харчова промисловість, фармацевтика, виробництво мікроелектронних виробів, робототехніка і багатьох інших.

Перші спроби змусити комп'ютер «бачити» відносяться до початку 60-х років 20 століття. Однак лише в останні роки в зв'язку з підвищенням обчислювальних потужностей і швидкодії процесорів, обсягів пам'яті, підвищенням роздільної здатності та інших параметрів камер, розвитком смуги пропускання каналів зв'язку, а також з появою таких технологій, як машинне глибоке навчання (Machine/Deep Learning) , штучний інтелект AI (Artificial Intelligence) технології CV/MV стали знаходити все більше застосувань в різних галузях промисловості і повсякденному житті людей [1].

На рис.1. показана одна з найпростіших промислових систем комп'ютерного зору - автомат для визначення ступеня повноти пляшки на лінії розливу напоїв. На основі аналізу зображення з фотокамери система здатна видавати тільки дві відповіді - повна пляшка, чи ні.

Перші спроби змусити комп'ютер «бачити» відносяться до початку 60-х років 20 століття. Однак лише в останні роки в зв'язку з підвищенням обчислювальних потужностей і швидкодії процесорів, обсягів пам'яті, підвищенням роздільної здатності та інших параметрів камер, розвитком смуги пропускання каналів зв'язку, а також з появою таких технологій, як машинне глибоке навчання (Machine / Deep Learning) ,

штучний інтелект AI (Artificial Intelligence) технології CV / MV стали знаходити все більше застосувань в різних галузях промисловості і повсякденному житті людей.

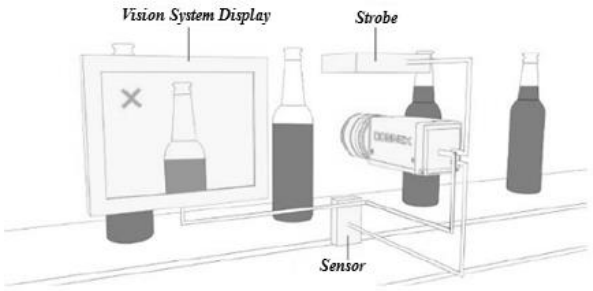


Рис. 1 - Приклад найпростішої систем комп'ютерного зору

Вважається, що перша ідея про те, щоб навчити комп'ютер бачити, виникла у професора MIT (Массачусетський технологічний інститут) Лоуренса Робертса (Lawrence Roberts), якого називають також одним із засновників Інтернету. Він першим створив системи розпізнавання форм предметів за допомогою комп'ютера, на чому захистив в MIT докторську дисертацію (PhD) [2]. В останні роки CV стало активно використовуватися в промисловості, в т.ч. в таких галузях, як автомобілебудування, харчова промисловість, фармацевтика і виробництво мікроелектронних виробів. Наприклад, в автомобілебудуванні транспортні засоби, як правило, включають безліч варіантів деталей, тому автовиробники застосовують системи CV, щоб зчитувати маркування компонентів при складанні на конвеєрі для того, щоб були встановлені саме потрібні в даній комплектації деталі. Крім того, CV необхідно для керування роботами на автоскладальному конвеєрі.

Комп'ютерне зір також використовується для підвищення якості, зокрема, для огляду, калібрування, перевірки розмірів, зазорів, відстаней, а також для вирівнювання деталей на лініях складання автомобілів.

У виробництві харчової продукції системи CV можуть перевіряти, чи всі інгредієнти вказані на упаковці товару, особливо ті, які можуть містити алергічні речовини. Нанесення штрих-кодів необхідно для швидкопсувних товарів, а код партії необхідний на випадок відкликання продукції з обігу. Системи машинного зору можуть забезпечити точний і гігієнічний безконтактний метод контролю рівня заповнення або розмірів готової продукції для відповідності рівню якості. Фармацевтика має на увазі високу відповідальність за забезпечення безпеки, тому необхідно надійно відслідковувати всі компоненти складу і якість готової продукції. При виготовленні мікросхем і електронних компонентів CV використовують в чистих

приміщеннях для контролю розміщення кремнієвих пластин, маркування та положення чіпа інтегральних схем та інших елементів. Більше 100 різних компаній, такі як Adani, Cognex, Viper Imaging, Applied Vision Corporation, Omron і інші почали виробляти системи машинного зору. Були розроблені спеціальні світлодіоди для систем машинного зору, розширювалися функції світлових сенсорів і архітектури управління системами CV. Це значно розширювало їх функціонал при постійному зниженні цін на такі системи.

Сьогодні комп'ютерний зір широко застосовується для багатьох компонентів цифрової економіки і в багатьох інших. Причому, постійно з'являються все нові області і сценарії застосування CV: «Розумне місто» (Smart City); Інтелектуальні транспортні системи ITC (Intelligent Transportation System); Автономні автомобілі (Driverless Car) і системи допомоги водієві ADAS (Advanced driver-assistance systems) ; Безпілотні літальні апарати (в т.ч. дрони); Високотехнологічне сільське господарство (Smart Agriculture); Електронна медицина (eHealth); Системи військового застосування; Аддитивное виробництво (3D-printing).

Література:

1. Техническое зрение роботов/'В. И. Мошкин, А. А. Петров, В. С. Титов, Ю. Г. Якушенков; Под общ. ред. Ю. Г. Якушенкова. —М.: Машиностроение, 2018. —272 с.: ил.

2. Borisov O.I., Gromov V.S., Pyrkin A.A., Bobtsov A.A., Nikolaev N.A., Robotic Boat Setup for Control Research and Education // IFACPapersOnLine.2016, V. 49, N. 6, P. 256–261.

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДИЗАЙНЕРСЬКІЙ ДІЯЛЬНОСТІ

Щерба Даніїл Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У даній статті розглядається питання використання інформаційних технологій у дизайнерській діяльності. На сучасному етапі суспільного розвитку інформаційні технології є обов'язковою складовою будь-якої сфери професійної діяльності. Не є винятком та професія дизайнера, для оволодіння якою абсолютно необхідні компетенції, пов'язані з використанням інформаційних технологій. У статті розглянуться базові інформаційні технології, що використовуються у дизайнерській діяльності.

Вступ

На сьогодні намітилася стійка тенденція, що зв'язує професійний рівень фахівця будь-якої сфери діяльності та його вміння застосовувати сучасні інформаційні технології, тобто орієнтуватися у великих обсягах інформації, обробляти

інформацію, використовуючи обчислювальну техніку та комп'ютерні мережі, освоювати сучасне програмне забезпечення. Це твердження повною мірою стосується та діяльності дизайнера, для якого знання широкого спектру інформаційних технологій є основним професійною вимогою. Сфери застосування інформаційних технологій в дизайні вкрай різноманітні, включають як безпосередню дизайнерську діяльність (роботу в графічних пакетах, створення анімованих кліпів, розробка тривимірної графіки та анімації, розробка відеокліпів, інтерфейсів веб-сторінок та інше), так та діяльність допоміжного характеру (роботу з офісними додатками, спеціалізованими базами даних, локальними та глобальними мережами).

Приблизний перелік програмно-технічних засобів забезпечення дизайнерської діяльності:

1. Векторні графічні редактори (Adobe Illustrator, Corel Draw, Adobe Image Ready, Inkscape);
2. Растрові графічні редактори (Adobe Photoshop, GIMP);
3. Програми для 3D-моделювання (Autodesk 3D Max, Autodesk Maya);
4. Програми для створення анімації та роботи з відео (Adobe Flash, Adobe After Effects, FireAlpaca, Sony Vegas);
5. Програми для створення мультимедійних презентацій (Microsoft Power Point, Adobe Director, Prezi, Lotus Freelance Graphics, Astound Presentation);
6. Інструментальні засоби розробки веб-сайтів (Adobe Dreamweaver, WordPress, Joomla, ModX, Wix);
7. Настільні видавничі системи (Microsoft Publisher, Adobe PageMaker, QuarkXPress, Corel Ventura, Adobe InDesign).

Основна частина

Розглянемо інформаційні технології допоміжного характеру, з якими доводиться взаємодіяти дизайнеру в процесі своєї щоденної роботи. Насамперед необхідно згадати найпопулярніші офісні прикладні програми - це програми пакета Microsoft Office.

Дизайнерська діяльність не обходиться без підготовки різних текстових документів, таких як звіти, оголошення, запрошення, різних типів ділової документації, що виконуються за допомогою текстового процесора Microsoft Word. Всі подібні документи є блоками тексту, що складаються зі звичайних та спеціальних символів, що включають малюнки, таблиці, виноски, колонтитули, нумерацію сторінок, змісту та ін. Microsoft Word дозволяє вводити фрагменти тексту,

застосовувати до них редагування та форматування, виводити документ або його частини на друк.

Microsoft Word дозволяє редагувати як текст, введений з клавіатури, так та розпізнаний, перетворений з графічного зображення, отриманий шляхом сканування. Процес редагування вихідного тексту включає різні операції, такі як додавання та видалення фрагментів тексту, зміна порядку частин документа, перевірка синтаксису та орфографії, виправлення помилок та інших операцій, які реалізуються в рамках програми Microsoft Word. Операції форматування тексту, що містять вибір шрифту, відстані між рядками, завдання полів, нового рядка, форматування абзаців, виділення заголовків та ін., визначають зовнішній вигляд документа. Найбільш популярними текстовими процесорами, крім Microsoft Word, є Multi-Edit, Lexicon, WordPerfect, Microsoft Works.

Табличними процесорами називають комп'ютерні програми, які призначені для зберігання та обробки даних, представлених в табличній формі. Самим широко поширеним табличним процесором є Microsoft Excel. Області застосування Microsoft Excel досить різноманітна. Електронні таблиці широко застосовуються в бухгалтерській, фінансовій, обліковій діяльності, використовуються для здійснення наукових та статистичних розрахунків, створення різних форм інфографічного подання інформації.

В сучасних умовах важливого значення набувають спеціалізовані програмні продукти, пов'язані з **управлінням проєктами**. У пакеті Microsoft Office присутній програма управління проєктами Microsoft Project, що являє собою систему управління проєктами та портфелями. Microsoft Project допомагає оптимізувати проєкти, ресурси та управління портфелем, а за допомогою засобів планування програма дає можливість відстежувати проєкти та тримати їх під контролем. Використання спеціальних інструментів планування та контролю дозволяє швидко приступити до роботи та спрощує реалізацію проєктів. Microsoft Project надає широкий спектр вбудованих шаблонів та інструментів планування, а також можливість доступу з різних пристроїв, що підвищує продуктивність роботи всіх учасників проєкту.

Також в діяльності сучасного дизайнера широко застосовуються телекомунікаційні технології, а саме - робота в глобальних та локальних комп'ютерних мережах, використання інформаційних ресурсів в мережі Інтернет та онлайн-сервісів,

таких як електронна пошта, телеконференції, відеозв'язок та інше.

Необхідно відзначити, що розвиток Інтернет-технологій призвів до формування таких нових галузей діяльності, як веб-дизайн та реклама в мережі Інтернет, можливості яких на сьогодні використовує велика кількість організацій в різних сферах діяльності.

Окремим напрямком діяльності дизайнера є розробка **мультимедійних презентацій**. У сучасній ситуації електронні презентації зайняли свою важливу нішу в повсякденній діяльності практично будь-якої організації в різних сферах. Професійно підготовлена презентація є невіддільною частиною діяльності будь-якої компанії, сприяє просуванню товарів та послуг на ринку, покращує імідж компаній, залучає нових клієнтів. Розвиток мультимедійних технологій сприяє максимально ефективному донесенню інформації до потенційного клієнта.

Електронна презентація, що поєднує в собі елементи каталогу, довідника, буклету, що включає відео-, аудіо-супровід та анімаційні ефекти, є сучасним способом подання інформації про саму компанію, товари та послуги. Електронні презентації можна поділити на ті, що забезпечують щоденну рутинну діяльність на робочому місці (супровід нарад, різних доповідей, звітів про виконану роботу) та виконують іміджеві та рекламні функції (мультимедіа презентації, поширювані на DVD або через Інтернет, розроблені професійними дизайнерами, які включають високоякісні ілюстрації та відеокліпи, що відрізняються сучасним дизайном та складними відеоефектами).

Іміджева мультимедійна презентація є сучасним ефективним способом подання корпоративної інформації, оскільки поєднує в собі елементи інтерактивності, відео, об'ємного звуку, тривимірної графіки. Іміджеві презентації використовуються для поширення інформації серед потенційних замовників, клієнтів та партнерів, є готовим рекламним продуктом з проробленим відеорядом, музичним супроводом, титрами, дикторським текстом.

Мультимедійний характер електронних презентацій дозволяє значно підвищити ефективність рекламування товарів та послуг. Ефект впливу від грамотно розробленої презентації виявляється зіставимо з ефектом від особистої консультації фахівця з продажу. Один компакт-диск з електронною презентацією може вміщати велику кількість текстової, графічної, відеоінформації, а також елементи анімації, аудіосупровід, спеціальні відеоефекти. Також електронна

презентація може входити до складу контенту корпоративного веб-сайту. Таким чином, мультимедійні презентації підвищують ефективність реалізації інформаційних та рекламних кампаній.

Сучасні засоби розробки презентацій дозволяють без знання програмування створювати та редагувати мультимедійні презентації. Однією з найбільш широко використовуваних програм в цій галузі є програма Microsoft PowerPoint з пакета офісних програм Microsoft Office. Такі характеристики даного програмного засобу, як простий та зручний інтерфейс, сумісність з іншими офісними додатками, наявність великої кількості шаблонів та стилів оформлення слайдів, бібліотека анімаційних ефектів, підтримка мультимедійних файлів, простота використання визначають популярність Microsoft PowerPoint.

У професійних дизайнерів мультимедійних презентацій великою популярністю користуються програма Adobe Flash та пакет Adobe Director Shockwave Studio, що володіють великими можливостями для створення ефектів анімації та інтерактивності.

Також існують спеціалізовані веб-сервіси, які дозволяють створювати презентації, що відповідають сучасним високим вимогам до дизайну та мультимедійних ефектів. Серед них можна виділити як найбільш популярні - програми Prezi, Lotus Freelance Graphics, пакет Astound Presentation. Prezi.com - це веб-сервіс, за допомогою якого створюються інтерактивні мультимедійні презентації. Робота веб-сервісу Prezi.com заснована на технології масштабування (наближення та видалення об'єктів). На відміну від презентації, виконаної в Microsoft PowerPoint, де презентація розбивається на слайди, в Prezi основні ефекти пов'язані не з переходом від слайда до слайда, а зі збільшенням окремих частин цього ж слайда.

Одним з найбільш популярних напрямків роботи дизайнера є робота в графічних програмах, які дають широкі можливості при розробці **колажів, логотипів, ескізів поліграфічної продукції** (рекламних оголошень, листівок, брошур, буклетів, каталогів, візиток та ін.), Дизайну веб-сайту, елементів мультимедійних презентацій.

Adobe Photoshop є потужним графічним редактором, що займає перше місце в рейтингу комерційних продуктів для редагування растрових зображень. Програма працює на основі всіх популярних операційних систем, включаючи macOS, Windows Phone, iOS та Android. Adobe Photoshop, використовується в поліграфії, веб-дизайн, при створенні анімацій та мультимедійних файлів. Графічний редактор працює

з власним форматом PSD, який легко конвертується в будь-який інший формат зображень.

Основна функціональна база Adobe Photoshop - палітра інструментів для роботи з цифровими зображеннями або просканованими фото. У перелік можливостей програми входить корекція кольору, згладжування дефектів, ретуш, додавання спеціальних ефектів, налагодження динамічного діапазону. Також набір функцій графічного редактора включає видалення об'єктів та ретушування фотографій; початок роботи за допомогою шаблону; фотомонтаж; пошарове створення елементів, частини яких зберігаються окремо; робота з текстовими блоками; застосування об'ємних текстур та фонів; обробка фотографій для публікацій або видруку; робота з ескізами.

Corel Draw - графічний редактор для роботи з векторною графікою, що розробляється корпорацією Corel. Поточною версією продукту є CorelDRAW Graphics Suite 2017, доступна тільки для Windows. Corel є передовим програмним забезпеченням для графічного дизайну, сучасним засобом для швидкого створення дизайн- та фотопроєктів, графіки та веб-сайтів. Corel Draw дозволяє зберігати об'єкти в різних графічних форматах, володіє унікальними функціями. Програмне забезпечення складається з декількох професійних модулів. Кожна частина виконує певну функцію. В одному модулі відбувається перетворення растрових зображень у векторний формат. Користувачі також можуть робити скріншот з екрана або окремої його частини. На додаток до цього дуже просто виконати обробку зображень, ретуш фотографій. Також є окремий модуль для розробки інтерфейсів веб-сайтів.

Також увагу слід приділити такому сучасному додатком для ілюстраторів, як Adobe Illustrator, яке орієнтоване на роботу з векторною графікою та дозволяє створювати логотипи, значки, малюнки, типографіку та ілюстрації для друкованих видань, веб-публікацій, відео та мобільних пристроїв. Дизайнери використовують Adobe Illustrator в різних цілях: в рекламі, вітальних листівках, плакатах, книгах, графічних романах, розкадрування, журналах та газетах. Програма володіє широким набором інструментів для малювання та можливостями управління кольором та текстом.

Настільні видавничі системи. Для рекламних повідомлень надзвичайно важливо створювати сильне початкове враження, що досягається засобами композиції, оригінальним кольорографічним рішенням, якістю та яскравістю контенту. Спектр рекламної продукції досить

широкий - від візиток та фірмових значків до рекламних каталогів та брошур. Часто для створення ескізів рекламних матеріалів використовуються настільні видавничі системи. Особливо це стосується сфери, пов'язаної з оперативної (малотиражною) поліграфією, при роботі в якій дизайнеру доводиться розробляти повноцінні макети поліграфічних видань за короткий проміжок часу.

Термін DeskTop Publishing System або «настільна видавнича система» з'явився в 80-х роках XX століття. На цей час настільні видавничі системи по суті є програмами електронної верстки документів, що дозволяють редагувати та форматувати текст, макетувати та верстати публікації, використовувати велику кількість шрифтів, обробляти графічні зображення, використовувати бібліотеки малюнків та шаблони оформлення, виводити публікацій поліграфічної якості на друк. Наразі широко поширеними видавничими системами є QuarkXPress, Corel Ventura, Adobe InDesign, Microsoft Publisher, Adobe PageMaker.

Мультимедійні технології в дизайні. Говорячи про походження терміна «мультимедіа», варто відзначити, що він походить від латинського слова "multum", що означає "багато", та "media" - кошти. Мультимедіа розглядається як "одночасне використання різних форм представлення інформації та її обробки в єдиному електронному об'єкті-контейнері". Прикладом мультимедійного продукту може виступати електронна презентація, яка містить текстову, аудіальну, графічну та відеоінформацію, а також елементи інтерактивності (взаємодії з користувачем).

Мультимедійні технології набули широкого поширення порівняно недавно завдяки зростанню технічних можливостей персональних комп'ютерів, таких як швидкодія, великі обсяги пам'яті, потужні звукові та відеокарти, а також появі та доступності нових носіїв інформації, таких як CD-, DVD-, BlueRay-диски, flash- карти, переносні сховища даних. На сьогодні мультимедійні технології використовуються в інформаційному забезпеченні різних сфер діяльності. Зокрема, за допомогою мультимедіа засобів створюється широкий спектр рекламної продукції - розробляються рекламні відеоролики, оформляються анімовані логотипи та банери, створюються мультимедійні презентації та іміджеві рекламні сайти.

Комп'ютерна анімація - це технології створення рухомих зображень з використанням спеціалізованого програмного забезпечення, що комбінують комп'ютерний малюнок та моделювання з рухом. Термін анімація походить від

англійського «animate», що означає «оживляти». На цей момент комп'ютерна анімація використовується в різних галузях: в традиційній мультиплікації, комп'ютерних іграх, відеофільми, рекламних роликах, Інтернет-сайт, електронних презентаціях.

Комп'ютерна анімація підрозділяється на двовимірну та тривимірну. Двовимірна графіка та анімація (2D) мають справу зі створенням зображень на площині, тоді як тривимірна (3D) графіка розробляє об'ємні (тривимірні) образи об'єктів.

Спектр професійних програмних засобів для створення анімаційних ефектів розширюється. До найбільш популярних програм, що дозволяють створювати двовимірну анімацію, відносяться Adobe Flash, Adobe Image Ready, Corel Real Animated Vector Effects, Ulead GIF Animator та інші. Для моделювання та анімації тривимірних об'єктів та середовищ використовуються такі програми, як 3D Studio Max, Maya, Adobe After Effects, Lightwave 3D, Blender, Bryce, Realsoft 3D.

Програма Adobe Flash є популярною мультимедійною платформою, яка розробляється компанією Adobe Systems для створення мультимедійних презентацій та веб-додатків, а також для створення рекламних банерів, ігор, анімації. Adobe Flash працює з різними типами графіки: векторної, растрової та тривимірної.

Autodesk 3ds Max (раніше 3D Studio MAX) - це програмне забезпечення для 3D-моделювання та візуалізації дозволяє створювати масштабні світи комп'ютерних ігор, вражаючі сцени для візуалізації проєктів та захоплюючу віртуальну реальність. 3ds Max є професійним програмним забезпеченням для створення та редагування тривимірної графіки та анімації, що містить просунуті засоби для дизайнерів та фахівців в області мультимедіа.

3ds Max володіє різноманітними засобами для створення різноманітних тривимірних комп'ютерних моделей з використанням таких технік та механізмів, як полігональне моделювання, моделювання за допомогою поверхонь Безьє, моделювання з використанням вбудованих бібліотек стандартних об'єктів (примітивів) та модифікаторів.

У даній статті було розглянуто базові інформаційні технології, що застосовуються у дизайнерській діяльності.

Конкурентоспроможність сучасного дизайнера безпосередньо залежить від того спектра інформаційних технологій, якими він зумів опанувати в процесі навчання, оскільки дизайн як професійна діяльність здебільшого перейшов у цифрову реальність. Професійному дизайнеру у своїй повсякденній діяльності доводиться мати справу з великою

кількістю інформаційних технологій, які зачіпають комп'ютерну графіку, мультимедійні технології (технології обробки відео- та аудіоінформації, комп'ютерна анімація), тривимірне моделювання, які використовуються при створенні друкованої реклами, реклами на радіо, телебаченні, реклами в мережі Інтернет, при розробці електронних мультимедійних презентацій.

Література:

1. E. Kalay Y. The impact of information technology on design methods, products and practices / Yehuda E. Kalay // Design Studies / Yehuda E. Kalay. – Berkeley, 2006. – С. 357–380.

2. What Is Design Innovation & Why You Need To Know It [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/codomo/what-is-design-innovation-why-you-need-to-know-it-b8d850503b3a.

3. 11 Best Graphic Design Software of 2021 (Free and Paid) [Електронний ресурс] – Режим доступу до ресурсу: https://www.adamenfroy.com/best-graphic-design-software.

СТАНДАРТ БЕЗДРОТОВОГО ЗВ'ЯЗКУ WI-FI 6

Юхименко Валентин Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Постановка задачі. Ознайомити слухачів із перспективами використання та розвитку Wi-Fi 6

Мета дослідження. Донести інформацію по темі, розділивши її на 4 пункти:

1) Що таке стандарт Wi-Fi 6?
2) Стандарт Wi-Fi 6 на практиці.
3) Переваги стандарту Wi-Fi 6.
4) Чого очікувати в найближчі роки?

Результати досліджень.

Стандарт Wi-Fi 6, також відомий як 802.11ax, - це нове покоління Wi-Fi і черговий крок на шляху безперервного впровадження інновацій. Спираючись на можливості стандарту 802.11ac, Wi-Fi 6 дозволяє підвищити швидкість передачі даних і пропускну здатність як нових, так і вже існуючих мереж при роботі з додатками нового покоління за рахунок збільшення ефективності, гнучкості і масштабованості. Стандарт Wi-Fi 6 був запропонований інститутом інженерів з електротехніки та електроніки (IEEE) з метою об'єднати широкі можливості і високу швидкість бездротових технологій Gigabit Ethernet з надійністю і передбачуваністю ліцензованої радіомережі.

Необхідність розробки нового стандарту була викликана зростанням числа клієнтських пристроїв. Кількість частотних каналів не змінюється, а продовжує ділити їх дедалі зростаючу кількість наших і сусідських гаджетів. У Wi-Fi 4 це був діапазон 2,4 ГГц, в Wi-Fi 5 - 5 ГГц. У маршрутизаторах з підтримкою обох режимів тимчасово була вирішена проблема кількості підключених девайсів, але все одно залишалися нюанси з покриттям і маршрутизацією даних. Головний упор в стандарті Wi-Fi 6 зроблений на оптимізацію передачі даних та інтелектуальне управління підключеннями клієнтських пристроїв .

В основу Wi-Fi 6 будуть покладені сильні сторони стандарту 802.11ac. При його використанні точки доступу зможуть підтримувати більшу кількість клієнтів в середовищах з високою щільністю, а робота в стандартних бездротових локальних мережах стане простіше. Крім того, він забезпечить більш передбачувану продуктивність сучасних додатків, таких як перегляд відео з роздільною здатністю 4K і 8K, додатків для спільної роботи з високою щільністю і високим дозволом, бездротового доступу в офісах і Інтернету речей (IoT). Оскільки бездротові технології розповсюджуються все ширше, саме Wi-Fi 6 визначить майбутнє мереж Wi-Fi.

Переваги:

a) Збільшена швидкість інтернету

За заявою творців новий стандарт забезпечує максимальну швидкість до 9,6 Гбіт / с, тоді як Wi-Fi 5 - до 6,77 Гбіт / с. Обіцяють, що роутер з підтримкою нового стандарту дасть приріст швидкості до одного підключеного пристрою на 40%, в порівнянні з Wi-Fi 5, і все завдяки новому типу кодування інформації і більш потужним чіпам в роутерах, які здатні впоратися зі збільшеним потоком даних.

b) Зменшене споживання енергії

Wi-Fi 6 отримав нову функцію Target Wake Time, яка покликана зменшити витрати енергії у підключених до мережі гаджетів. А відбувається це так: Target Wake Time аналізує кожен пристрій в зв'язці і визначає, чи потрібно йому зараз підключення або користувач робить щось інше. У другому випадку функція тимчасово відключає Wi-Fi-модуль і економить заряд акумулятора, поки той не знадобиться знову, знижуючи енергоспоживання до семи раз. Зрозуміло, що це сильно збільшує термін служби батареї.

c) Безпека даних в Wi-Fi 6

Новий стандарт Wi-Fi дозволяє використовувати в роутерах шифрування WPA3. Розрядність шифрування

розширена до 192 біт (в порівнянні з WPA2 з його 128-бітами), що сприятливо позначається на захисті слабких паролів, які в разі мереж п'ятого покоління зловмисники можуть зламати за лічені секунди. Стандарт безпеки WPA3 також оберігає дані підключених користувачів в громадських місцях і мережеві пристрої від злому.

Уже деякий час виробники мережевого обладнання пропонують свої пристрої з підтримкою Wi-Fi 6. Гаджети також не відстають і, наприклад, ті ж смартфони, починаючи з iPhone 11 і Samsung Galaxy Note 10, отримали підтримку Wi-Fi 6. Нікуди не дітися від проблем при впровадженні технології, як це досі спостерігається для Wi-Fi 5. Роутер з Wi-Fi 6 не забезпечить ноутбуку минулих років поліпшеного сигналу в віддаленій точці і швидку передачу всередині мережі. Оновлювати потрібно буде весь парк пристроїв. Не варто забувати, що ефект від «швидше-вище-сильніше» помітний для випадків з дійсно інтенсивним навантаженням. Якщо до маршрутизатора з Wi-Fi 6 підключені пара смартфонів і ноутбук з Wi-Fi 6, різниця в швидкості буде малопомітна. Саме тому в Альянсі говорили, що новий стандарт, перш за все, розрахований на вирішення проблем в місцях масового скупчення - ресторанах, стадіонах, парках, торгових центрах і т.д.

Висновки та перспективи

Зростанню ринку чіпсетів Wi-Fi 6 сприятиме цілий ряд факторів, серед яких безпрецедентне зростання пристроїв, оснащених Wi-Fi, і пристроїв з підтримкою різних типів інформаційних каналів і трафіку; збільшення показника «число користувачів на точку доступу»; висока щільність покриття Wi-Fi-мереж; зростання використання зовнішніх мереж Wi-Fi (поза приміщеннями), а також бажання підвищити енергетичну та спектральну ефективність прийому-передачі. В результаті перспективи підвищення продуктивності пристроїв в щільній мережевому середовищі зробили Wi-Fi 6 головною новою тенденцією в побудові мереж бездротового зв'язку і бізнес-додатків.

Література:

1. *https://hi-tech.ua/article/wi-fi-6-overview/*
2. *https://www.cisco.com/c/ru_ru/products/wireless/what-is-wi-fi-6.html*
3. *https://ru.wikipedia.org/wiki/IEEE_802.11ax*
4. *https://root-nation.com/ru/posts/tech/ru-what-is-wi-fi-6-differences/*

Янішевський Олексій Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Коли ми говоримо про віртуальну реальність, багато хто з нас думає про науково-фантастичні фільми. Однак правда полягає в тому, що в наш час ця технологія повністю поєднується з нашим повсякденним життям. Відеоігри, медицина, освіта… Віртуальна реальність тут і зараз. Але що саме вона собою представляє?

Віртуальна реальність (VR) - це комп'ютерно-згенероване середовище, де сцени та об'єкти здаються справжніми, завдяки чому користувач відчуває, що занурений у цей світ. Це середовище сприймається через пристрій, відомий як гарнітура або шолом віртуальної реальності. VR дозволяє нам зануритися у відеоігри так, ніби ми є одним із персонажів, навчитися виконувати операції на серці або покращити якість спортивних тренувань.

Хоча це може здатися надзвичайно футуристичним, походження цієї технології не настільки недавнє, як ми гадаємо. Насправді багато людей вважають, що одним із перших пристроїв віртуальної реальності називали Sensorama, машину із вбудованим сидінням, яка відтворювала 3D-фільми, видавала запахи та генерувала вібрації, щоб зробити досвід максимально яскравим. Винахід датується серединою 1950-х років.

Завдяки множині нових апаратних та програмних можливостей, майбутнє носимих пристроїв швидко розгортається. Такі пристрої, як HTC Vive Pro Eye, Oculus Quest та Playstation VR, безумовно є лідерами, але є й такі гравці, як Google, Apple, Samsung, Lenovo та інші, які можуть здивувати галузь новими рівнями занурення та зручностями використання. Хто б не вийшов уперед, простота придбання пристрою розміром із шолом, який може працювати у вітальні, офісі чи на заводській підлозі, зробила технологію доступнішою.

Не дивно, що індустрія відеоігор є одним з найбільших прихильників Віртуальної реальності. Підтримка гарнітур Oculus Rift вже була запрограмована на такі ігри, як Skyrim і Grand Theft Auto, але нові ігри, такі як Elite: Dangerous, мають вбудовану підтримку гарнітури. Багато елементів інтерфейсу користувача в іграх повинні бути з урахуванням віртуальної реальності (зрештою, хто хоче вибирати елементи з меню, яке займає все ваше поле зору?), але галузь швидко адаптується, оскільки обладнання для справжніх ігор у віртуальну реальність стає все більш доступним .

Наукова та інженерна візуалізація даних роками отримувала вигоду від віртуальної реальності, хоча останні інновації в технології відображення викликали інтерес до всього, починаючи від молекулярної візуалізації, закінчуючи архітектурою та моделями погоди.

В авіації, медицині та військовій галузі навчання з віртуальної реальності є привабливою альтернативою тренуванням у прямому ефірі з дорогим обладнанням, небезпечними ситуаціями або чутливими технологіями. Комерційні пілоти можуть використовувати реалістичні кабіни з технологією VR у цілісних навчальних програмах, що включають віртуальний політ та навчання в режимі реального часу. Хірурги можуть тренуватися за допомогою віртуальних інструментів та пацієнтів, а також переносити свої віртуальні навички в операційну, і дослідження вже почали показувати, що таке навчання призводить до лікарів, які оперують швидше і роблять менше помилок. Поліція та солдати можуть проводити віртуальні тренування по зачистці території, щоб уникнути ризику для життя.

Говорячи про медицину, лікування психічних захворювань, включаючи посттравматичний стресовий розлад, має переваги від використання технології віртуальної реальності для постійних програм терапії. VR має потенціал, що перевищує ігрові, промислові та маркетингові програми, щоб допомогти людям вилікуватися, узгодити та зрозуміти реальний досвід.

Література:
1. *https://www.marxentlabs.com/what-is-virtual-reality/*
2. *https://www.iberdrola.com/innovation/virtual-reality*

ШЛЯХИ ТА МЕТОДИ ЗАХИСТУ ОПЕРАЦІЙНОЇ СИСТЕМИ LINUX

Яцунський Олександр Русланович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Щодня виявляються десятки вразливостей, створюються сотні експлойтів. Не виключено, що вразливість може бути знайдена і в UNIX-системах, тому, вам варто убезпечити себе від «небажаного вторгнення».

Linux є операційною системою з відкритим вихідним кодом. Існує багато дистрибутивів операційних систем на основі Linux, таких як Red Hat, Fedora та Ubuntu. На відміну від інших операційних систем, Linux менш безпечний. Це пов’язано

з тим, що вихідний код доступний безкоштовно, тому його легко вивчити на наявність слабких місць і використовувати їх в порівнянні з іншими операційними системами, що не мають відкритого коду.

Захист інформації в конкретній операційній системі нерозривно пов'язаний з завданнями, для вирішення яких застосовується дана ОС. Unix-подібні операційні системи, і, зокрема, Linux, спочатку використовувалися в якості мережевих ОС на серверах локальних обчислювальних мереж. І зараз за статистикою проекту Netcraft приблизно 93% серверів в мережі Інтернет працюють під управлінням таких операційних систем. Серед останніх чималу частину складають різні модифікації Linux.

Деякі користувачі переконані в тому, що Linux абсолютно захищена відразу після установки і не потрібні ніякі додаткові заходи, спрямовані на збільшення її безпеки. Як один з варіантів подібного оману існує думка, що «вірусів під Linux не буває». Відсутність вірусів пояснюють особливостями архітектури системи, яка робить їх існування неможливим. Віруси та інші шкідливі програми під Linux зустрічаються , хоча і не в такій кількості, як під ОС сімейства Windows.

Особливістю шкідливих програм під Linux є те, що для початку своїх деструктивних дій вони вимагають прямого втручання користувача. Мимовільної активації вірусу без участі користувача (звичайна ситуація в Windows, наприклад, в разі вірусів MSBlast і NetSky) не відбувається. Таким чином, мала кількість вірусів пояснюється слабкою поширеністю Linux саме в якості операційної системи для призначеного для користувача комп'ютера.

Друга досить поширена помилка відноситься не тільки до систем на базі Linux: багато користувачів чомусь впевнені, що саме їх сервер ніхто не стане зламувати. Якщо ваш сервер або робоча станція в мережі до сих пір не піддавалися зловмисному впливу, це не означає, що і в майбутньому ніхто не зробить подібних спроб. Навіть якщо на сервері немає ніяких важливих даних, захоплений сервер можна використовувати для розсилки спаму або для організації атак на інші сервери.

Існують багато методів, які допоможуть захистити вашу ОС як найкраще, такі як:

1. Регулярні оновлення
2. Підвищення привілеїв і контроль цілісності
3. Захист мережі

4. Захист поштового сервера

Система виявлення вторгнень

- **Fail2ban** - демон, який можна використовувати для захисту вашого сервера від атак методом перебору паролів (Brute Force). Одним з головних завдань Fail2ban є блокування IP-адреси, активність якого має явні шкідливі ознаки. Всі фільтри і дії налаштовуються в файлах конфігурації, таким чином Fail2ban є відмінним гнучким інструментом для запобігання злому.
- **Snort** - це програмне забезпечення для виявлення спроб вторгнення з мережі. Він є одним з найулюбленіших інструментів адміністраторів і головним фігурантом багатьох посібників з безпеки. Snort можна і не конфігурувати, тому що стандартних налаштувань більш ніж достатньо для захисту типових мережевих сервісів.
- **Tripwire** – один із кращих інструментів для забезпечення безпеки Linux. Це система виявлення вторгнень (HIDS). Завдання Tripwire – моніторинг файлової системи і фіксування змін файлів.
- **Rkhunter (Rootkit Hunter)** – це простий, але ефективний інструмент зі своєю базою, який сканує руткіти, бекдори і можливі локальні експлойти.

Завдяки переліченим вище методам захисту Linux, на вашому комп’ютері.

Коли справа доходить до безпеки, краще перестрахуватися спочатку, ніж шкодувати про це після. Новий спосіб злому, або шкідливе ПЗ - питання часу. Існує безліч хакерів, охочих дістати ваші особисті дані. Завдяки переліченим вище методам безпека ОС Linux буде набагато збільшена.

Література:

1. *https://news.netcraft.com/archives/category/web-server-survey/*
2. *https://github.com/Cisco-Talos/snort-faq/blob/master/README.md*

БЕЗПЕКА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Агапевич Назарій Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Безпеку інформаційно-телекомунікаційних технологій (безпека ІТТ) (ICT security): Всі аспекти, пов'язані з визначенням, досягненням і підтримкою конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності і достовірності інформаційно-телекомунікаційних технологій.

Для створення ефективної програми безпеки ІТТ фундаментальними є наступні високорівневі принципи безпеки:

- Менеджмент ризику - активи повинні бути захищені шляхом прийняття відповідних заходів. Захисні заходи повинні вибиратися і застосовуватися на підставі відповідної методології управління ризиками, яка, виходячи з активів організації, погроз, вразливостей і різних впливів загроз, встановлює допустимі ризики і враховує існуючі обмеження;
- Зобов'язання - важливі зобов'язання організації в області безпеки ІТТ і в управлінні ризиками. Для формування зобов'язань слід роз'яснити переваги від реалізації безпеки ІТТ;
- Службові обов'язки і відповідальність - керівництво організації несе відповідальність за забезпечення безпеки активів. Службові обов'язки і відповідальність, пов'язані з безпекою ІТТ, повинні бути визначені і доведені до відома персоналу;
- Мети, стратегії і політика - управління ризиками, пов'язаними з безпекою ІТТ, має здійснюватися з урахуванням мет, стратегій і політики організації;
- Управління життєвим циклом - управління безпекою ІТТ повинно бути безперервним протягом усього їх життєвого циклу.

Безпека ІТТ - це багатопланова організація процесів захисту, яку можна розглядати з різних точок зору. Взаємозв'язок компонентів безпеки, що показує, як активи можуть бути під впливом декількох загроз, одна з яких є основою для моделі. Набір загроз постійно змінюється і, як правило, відомий тільки частково. Також з часом змінюється і навколишнє середовище, і ці зміни здатні вплинути на природу загроз і ймовірність їх виникнення.

Модель безпеки відображає:

− навколишнє середовище, що містить обмеження і загрози, які постійно змінюються і відомі лише частково;
− активи організації;
− уразливості, властиві даними активами;
− заходи для захисту активів;
− прийнятні для організації залишкові ризики.

Після встановлення цілей безпеки ІТТ організації повинні бути розроблені стратегії безпеки ІТТ, є фундаментом розвитку політики безпеки ІТТ організації. Розвиток безпеки ІТТ необхідно для того, щоб гарантувати достовірність і ефективність результатів процесу управління ризиками. Для розвитку та успішної реалізації політики безпеки ІТТ в організації потрібно забезпечити її всебічне управління. Важливо, щоб політика безпеки ІТТ враховувала цілі і особливості даної організації. Політика безпеки ІТТ повинна об'єднуватися з політикою безпеки і бізнес-політикою організації. Таке об'єднання допоможе досягти найбільш ефективного використання ресурсів і забезпечити узгоджений підхід до безпеки в різних умовах навколишнього середовища.

Може виявитися необхідним розвивати окремі специфічні аспекти політики безпеки для кожної або декількох ІТТ. Ці напрямки повинні базуватися на оцінці ризику і узгоджуватися з політикою безпеки ІТТ, тим самим враховуючи рекомендації з безпеки для тих систем, з якими вони пов'язані.

Література:
1. https://www.rts-tender.ru/poisk/gost/r-isomek-13335-1-2006

БЕЗПЕЧНЕ ОНОВЛЕННЯ ПАРОЛЮ

Алексеєнко Олександра Анатоліївна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

У наш час людям необхідно створювати все більше і більше акаунтів: для пошти, для банку, на сайтах з комунальних платежів тощо. Всі вони потребують паролів і бажано різних. Через це виникає проблема забування, плутанини або виникнення підозрілої активності. Особливо в останньому випадку виникає необхідність провести скидання, тобто оновлення паролю, задля повернення безпеки власних та конфіденціальних даних. Отже, питанням тези буде розгляд безпечного оновлення паролю.

В базі даних паролі зберігаються зазвичай в одному з трьох основних видів:

1. *Звичайний текст.* Є таблиця з паролем, яка зберігається в звичайному текстовому вигляді.

2. *Зашифрований.* Зазвичай виконується симетричне шифрування, але зберігаються паролі теж в одному стовпці.

3. *Хешованні.*

Насамперед, необхідно чітко зазначити: ні в якому разі не зберігати паролі в простому вигляді. Одна неакуратна дія, маленька вразливість до ін'єкції і все – всі паролі клієнтів, від тих, чию безпеку ви забезпечуєте, до тих, які знаходяться в їх власному зберіганні, стануть надбанням суспільності.

Щодо шифрування є декілька питань. Основна його проблема – дешифрування. Взявши текст шифрування та повернувши його до нормального вигляду, ми отримуємо ситуацію, де пароль знову стає звичайним і шифрування втрачає сенс.

Ідея хешування полягає у тому, що воно виконується в одну сторону, тому єдиним способом зрівняти введений користувачем пароль з його хешованою версією – хешування введеного та їх порівняння. При правильній організації цього процесу можна бути впевненим, що паролі, які були хешовані, не стануть простим текстом.

Коли користувач просить «нагадати» пароль, адміністратору безпеки, по-перш за все, треба розуміти, що все що від нього необхідно – повернути користувача в онлайн. Звичайно, можна відправити пароль через пошту, та треба пам'ятати, що електронна пошта – це наднебезпечний канал зв'язку, якій до того ж зберігає дані на накопичувачі, до якого має доступ системний адміністратор, вона пересилається та розповсюджується, є доступною до шкідливого ПО. Тобто пошта не є нашим шляхом. Також, у разі хешування паролів у адміністратора безпеки є лише його хешована форма, що у разі «нагадування» не спрацює. Тому єдиним способом є: оновлення паролю.

Є два популярних шляхи оновлення паролю:

1. Генерація нового паролю та його відправка за допомогою пошти.
2. Відправка електронного листа з унікальнім URL-посиланням, що повинен полегшити процес оновлення.

Перший спосіб хоч і має низку прикладів та рішень, проте суперечить твердженням зазначеним вище. Коротко кажучи, він створює ситуацію, в якій пароль зберігається у простому вигляді. З'являється ймовірність блокування облікового запису із злим наміром. Якщо зловмиснику відома електронна пошта користувача, який має обліковий запис на веб-сайті, то йому легко в будь-який час заблокувати акаунт чи оновити пароль – відмова в обслуговуванні у чистому вигляді.

Говорячи про оновлення за допомогою URL, мається на увазі адреса веб-сайту, яка є унікальною для цього випадку. Він має бути випадковим та не мати в собі зовнішніх посилань на обліковий запис. Нам необхідно створити такий унікальний токен, який можна відправити поштою, а потім зіставити його з записом на сервері з обліковим записом користувача, таким чином підтверджуючи, що власник акаунту і є тією самою людиною, яка намагається виконати оновлення паролю.

Окрім цього, цей процес має забезпечувати лімітований час виконання оновлення та одноразовість. Короткий час забезпечує мале вікно, під час якого зловмисник має змогу провести свої маніпулювання. Після завершення процесу токен необхідно видалити, щоб URL більше не був працюючим.

Розмовляючи про оновлення паролю, необхідно розглянути також і секретні питання та відповіді, які є поширеним інструментом ідентифікації.

Проблема скидання паролю має стовідсоткову залежність від електронної пошти, тому що цілісність облікового запису, пароль якого необхідно оновити, залежить від цілісності пошти. Зловмисник, що має доступ до пошти користувача разом з нею має доступ до будь-якого акаунту, що був прив’язаний до пошти. Разом з цим він має можливість запросто скинути цей обліковий запис простим повідомленням на пошту.

Одним із способів попередити такий ризик – реалізувати секретні питання та відповідь. Вони дають змогу упевнитися, що людина, яка намагається оновити пароль, справді є власником цього облікового запиту.

Коли справа стосується секретних питань, то користувача необхідно врятувати від самого себе. Тобто, секретне питання повинно назначатися самим веб-сайтом, а ще краще, якщо цих питань буде декілька. Так у користувача з’являється можливість вибрати підходяще йому питання, а краще декілька, які потім будуть використані як допоміжний канал ідентифікації.

Декілька питань підвищують рівень впевненості в процесі перевірки, а також додає випадковості.

Яке секретне питання буде якісним? На це впливає декілька чинників:

1. Питання має бути коротким, чітким та однозначним.
2. Відповідь на питання має бути конкретною, аби позбутися можливою випадковості відповіді.
3. Множина можливих відповідей повинна бути великою, тобто вони повинні бути якомога унікальнішими для кожного користувача.

4. Пошук відповідей повинен бути складним для зловмисника. Вони як мінімум, не має включати в себе основу біографічну інформацію користувача.

5. Відповідь на питання має бути актуальною для користувача завжди. Отже назва улюбленого фільму під цей пункт не підпадає, адже смаки людині змінюються.

Ще одним аспектом, який потрібно розглянути щодо відповіді на секретне питання, є зберігання. Знаходження в ДБ простого тексту представляє майже ті ж загрози, що і в разі пароля, а саме: розкриття бази даних миттєво розкриває значення і піддає ризику не тільки сам додаток, але і потенційно абсолютно інші функції, які від нього залежать, наприклад, ті ж самі секретні питання.

Одним з варіантів є безпечне хешування, проте на відміну від більшості випадків зберігання паролів, тут може бути поважна причина видимості відповіді як простого тексту. Типовим сценарієм є перевірка особистості живим оператором по телефону.

Остання можлива проблема, що пов’язана із секретним питанням та відповіддю – це те, що вони вразливі перед соціальної інженерією. Намагатися безпосередньо випитувати пароль до чужого облікового запису – це одна справа, а зав'язати розмову про його освіту (популярний секретне питання) – зовсім інше.

Насправді, користувач цілком реально буде спілкуватися з кимось про якісь визначні аспекти його життя, які можуть представляти секретне питання, і не викликати при цьому підозр. Зрозуміло, сама суть секретного питання в тому, що він пов'язаний з чиїмось життєвим досвідом, тому він і можливий до запам’ятовування, і саме в цьому полягає проблема – людям подобається розповідати про свій досвід.

З цим мало що можна вдіяти, тільки якщо вибрати такі варіанти секретних питань, щоб їх з меншою ймовірністю можна було б витягнути соціальним інжинірингом.

Література:

1. «Good Security Questions» / [Електронний ресурс] – Режим доступу: http://goodsecurityquestions.com/

2. «Все, что вы хотели знать о безопасном сбросе пароля» / [Електронний ресурс] – Режим доступу: https://habr.com/ru/company/vdsina/blog/523690/

MITRE ATT&CK

Андрущенко Катерина Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Корпорація MITRE – це американська приватна некомерційна організація, яка співпрацює з приватними організаціями та урядом США. Їх мета – вирішувати проблеми, щоб зробити світ більш безпечним. MITRE ATT&CK – це всесвітньо доступна база знань щодо тактик і методів злочинців, заснованих на спостереженнях у реальному світі. База знань ATT&CK відкрита і доступна будь-якій особі чи організації для використання безкоштовно.

ATT&CK – структурований список відомих варіантів поведінки зловмисників, зібраний в тактики і методи, і виражений у вигляді таблиць, а також доступний у форматі STIX / TAXII. Оскільки цей список являє собою досить повне уявлення про поведінку зловмисників при компрометації мереж, він корисний для різних наступальних і захисних вимірювань, уявлень і інших механізмів [1].

Матриця ATT&CK складається з тактик, технік і процедур, також відомих як TTP. Графа тактик показує кроки, які зловмисник зазвичай використовуватиме з моменту отримання доступу до системи або мережі до виконання своєї мети.

Техніки розташовуються під тактиками і показують специфічні тактики, які зловмисник використовуватиме протягом атаки. Набір технік певної атаки також відомий як профіль поведінки для заданої атаки. Процедури містять деталі обраної техніки, приклади використання та методи протидії.

ATT&CK має декілька частин: PRE-ATT&CK, яка зосереджена на розвідці та налаштуванні інфраструктури, ATT&CK for Enterprise, яка охоплює корпоративні IT-мережі та хмари, та ATT&CK for Mobile, яка зосереджена на мобільних пристроях [2].

Матриця для підприємств містить інформацію про наступні платформи: Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office 365, SaaS.

Матриця для мобільних пристроїв містить інформацію про платформи Android та iOS. MITRE ATT&CK також включає в себе базу даних відомих злочинних угрупувань із загальною інформацією про них, даними про тактики та програмне забезпечення, яке вони використовують.

Отже, перелік тактик і технік в MITRE ATT&CK є досить вичерпним представленням кроків, які зловмисники використовують при компрометації мереж і систем, тому матриця MITRE ATT&CK корисна для планування захисту мереж і систем від кіберзагроз.

Література:

1. Что такое MITRE ATT&CK и как ее использовать [Електронний ресурс] – Режим доступу : https://blog.tiger-optics.ru/2018/12/what-is-mitre-attack/.

2. What Is MITRE ATT&CK? [Електронний ресурс] – Режим доступу : https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful.

PR В ІНТЕРНЕТІ

Андрущенко Катерина Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

PR (Public Relations) в інтернеті має не менш важливе значення, ніж в традиційних ЗМІ. PR в інтернеті призначений для створення позитивного іміджу компанії, її привабливого для споживачів образу. Традиційний PR включає співпрацю з друкованими виданнями, телевізійними каналами, радіо-станціями. Але сьогодні не можна не враховувати і ще один інформаційний канал - інтернет, тому PR в інтернеті активно доповнює PR в «офлайнових» ЗМІ.

Використання Інтернету PR-спеціалистами в майбутньому активізується, і станеться це, зокрема, з трьох причин:

1. Потреба в освіті проти потреби в продажах. Сьогоднішні споживачі розумніші, більш освічені. Вони можуть легко виявити підбурювачів і шахраїв. Таким чином, комунікаційні програми повинні грунтуватися на освітній інформації, а не на простому просуванні товарів і послуг. Ймовірно, Інтернет є найбільшим світовим джерелом такої інформації.

2. Потреба в роботі в режимі реального часу. Світ міняється дуже швидко. Усе відбувається миттєво, в режимі реального часу. PR -спеціалисти можуть використовувати це для своєї вигоди, з тим щоб структурувати інформацію для миттєвої реакції на виникаючі проблеми і зміни на ринку.

3. Потреба підлаштовуватися під клієнтів. Раніше існували три основні телевізійні мережі. Сьогодні - більше 500 телевізійних каналів. Сучасні споживачі чекають більш сфокусованих, цільових, індивідуальних взаємин. Все частіше і гущавині організації вимушені доводити свої повідомлення до зведення усе більш вузьких сегментів громадськості [1].

Взаємодія з інтернет-аудиторією може бути організована кількома шляхами: через соціальні сервіси і ресурси, через авторитетні інтернет-ЗМІ, через власний сайт компанії.

Не секрет, що соціальні мережі, популярні особисті та корпоративні блоги, форуми істотно впливають на формування громадської думки щодо тих чи інших подій, явищ. Тому PR в інтернеті обов'язково включає взаємодію з подібними соціальними сервісами.

У соціальній мережі компанія може організувати власну групу, що представляє її інтереси. Залежно від налаштувань кожної конкретної соціальної мережі, компанія зможе додавати з свою групу зображення (наприклад, фотографії реалізованих товарів або ж успішно виконаних проектів), публікувати новини

і замітки про життя компанії, організовувати обговорення новинок пропонованого асортименту, влаштовувати конкурси, рекламні акції.

Участь компанії в популярному тематичному форумі, відповідному профілю її діяльності, дозволить компанії з позиції експерта давати поради іншим учасникам такого форуму, відповідати на їхні запитання. Грамотні, ввічливі і компетентні повідомлення в цьому випадку формують у відвідувачів форуму стійке позитивне враження про компанії, а, власне, це і є основна мета PR в інтернеті.

Ще один важливий інструмент PR в інтернеті для компанії - це власний сайт. Це може бути представницький сайт або ж корпоративний, інтернет-магазин або ж рекламний промо-сайт. Кожен з типів сайтів допомагає реалізувати певне коло завдань PR, що стоять перед компанією [2].

Література:

1. Сучасні інформаційно-комунікаційні технології : навчальний посібник / [Г.Г.Швачич, В.В.Толстой, Л.М.Петречук та ін.] – Дніпро: НМетАУ, 2017. –230 с.

2. PR в інтернеті [Електронний ресурс] – Режим доступу : http://webstudio2u.net/ru/internet-ad/456-internet-pr.html.

СИСТЕМА УПРАВЛІННЯ ВМІСТОМ (CMS)

Андрущенко Катерина Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

З розвитком WWW "ручні" технології створення і підтримки сайтів вже не відповідали вимогам часу, а витрати на такі сайти були дуже істотними. Користувачів все більше цікавила можливість управляти сайтом: редагувати налаштування, додавати, створювати і правити контент, не удаючись до послуг професійних програмістів. Сучасний сайт - це вже не просто набір сторінок з посиланнями між ними, а повноцінний програмний продукт, який відстежує дії користувачів, дозволяє їм між собою спілкуватися і пропонує безліч корисних сервісів залежно від поставлених власником сайту завдань.

CMS - це програма, що надає інструменти для редагування (додавання, видалення інформації) і управління вмістом сайту, при цьому користувачеві не обов'язково мати навички програмування або знання мови HTML. CMS - це програмне забезпечення для організації веб-сайтів або інших інформаційних ресурсів в Інтернеті або окремих комп'ютерних мережах. Абревіатура «CMS» з'явилася від англійської фрази Content Management System, що і перекладається як система управління контентом.

У системі управління вмістом можуть знаходитися найрізноманітніші дані: документи, фільми, фотографії, номери телефонів, наукові дані і так далі. Така система часто використовується для зберігання, управління, перегляду і публікації документації. Контроль версій є однією з основних її переваг, коли вміст змінюється групою осіб. Системи управління контентом вирішують завдання адміністрування, управління і функціональності [1].

Актуальність розробки систем управління сайтом обумовлена необхідністю автоматизувати процес роботи з сайтом. Оперативне оновлення, додавання, видалення, редагування змісту, налаштування модулів системи повинні виконуватися не розробниками, а людьми, чиї пізнання в IT можна охарактеризувати як "користувач ПК", тобто співробітниками компанії [2].

Перші CMS були розроблені у великих корпораціях для організації роботи з документацією. У 1995-му від компанії CNET відокремилася окрема компанія Vignette, яка поклала початок ринку для комерційних CMS. З часом діапазон продукції розширювався і усе більш інтегрувався в сучасні мережеві рішення аж до популярних порталів веб. Багато сучасних CMS поширюються як безкоштовні і легкі у встановленні (інсталяції) програми, які розробляються групами ентузіастів під ліцензією GNU/GPL [1].

Основне завдання будь-якої системи управління полягає в тому, щоб об'єднати і організувати роботу з різними джерелами інформації в єдине ціле. Ці джерела інформації можуть розташовуватися всередині самого сайту або перебувати на сторонніх ресурсах. Також система управління може забезпечити взаємодію різних співробітників проекту і істотно полегшує процес управління, редагування та розміщення інформації на сайті.

Незважаючи на різноманітність систем управління, можна виділити загальні переваги, якими вони володіють:

1. Застосування систем управління дає можливість власнику ресурсу самостійно створювати, редагувати і видаляти розділи сайту і додавати інформацію без глибоких пізнань в веб-розробці.

2. Завдяки використанню CMS можна істотно прискорити і здешевити роботу з сайтом.

3. За рахунок того, що тимчасові витрати на створення багатьох елементів сайту знижуються, веб-майстер може більше часу приділити інформаційній складовій проекту і його дизайну [3].

Функції прикладних програм управління контентом:

− Створення контенту. Це сукупність завдань, які виконують автори текстів, фотографи, графічні художники, відео продюсери і звукорежисери, маркетингові експерти, юристи і інші люди, які подають оригінальний матеріал для користувачів веб-сторінки;

− Збір і адаптація контенту з існуючих джерел;

− Класифікація і індексування контенту. Контент має бути описаний формальними ознаками (наприклад, дата створення, автор) і класифікаційними даними (наприклад, предметна категорія або ключові слова). Така діяльність описується як зв'язка контенту і метаданих;

− Перегляд контенту. Необхідний для усіх видів опублікованого контенту;

− Затвердження. Формальне затвердження опублікованого контенту - важлива складова правової відповідальності за нього;

− Перетворення контенту. Тексти, графіка, звуки і інші форми контенту мають бути надані у форматі, який є найзручнішим або використовується в цій CMS;

− Зберігання контенту. Контент, як правило, зберігається у файлах або в БД. У разі складніших застосувань контент підлягає управлінню версіями програмного забезпечення (CMS);

− Тестування і верифікація контенту;

− Перевірка готовності контенту - це тип тестування, який включає верифікацію (перевірку) завершеності і цілісності великого об'єму контенту (наприклад, інформацію про різні аспекти нової послуги);

− Публікація. Враховує усі фізичні аспекти публікації контенту, включаючи дублювання контенту на різних серверах;

− Підтримка, актуалізація і контроль за змінами. Включає моніторинг опублікованого контенту і реагування на сигнали і необхідність змін;

− Відновлення і архівація;

− Звіти і аналіз. Включає різні форми звітності і аналізу, з метою кращого обслуговування користувачів, поліпшення виду порталу;

− Надання інструментів для створення утримуваного, організація спільної роботи над вмістом;

− Управління вмістом: зберігання, контроль версій, дотримання режиму доступу, управління потоком документів і тому подібне;

− Представлення інформації у виді, зручному для навігації, пошуку.

Принцип роботи CMS заснований на розподілі дизайну сайту і його вмісту. Зазвичай дизайн сайту міняється рідко, тоді, як зміни контенту можуть відбуватися не лише щодня, але і навіть кожну годину. Тому у своїй роботі CMS використовують так звані шаблони - спеціальні "порожні" сторінки, в яких дизайн сайту вже прописаний і залишилося лише наповнити їх інформацією. Користувач далекий від веб-дизайну і веб-програмування з легкістю може змінити зовнішній вигляд сайту, простою заміною одного шаблону на інший, при цьому контент залишиться. Проте, привілей розробляти шаблони залишилася за програмістами, оскільки цей процес вимагає певних спеціальних знань мов програмування.

Саме інформаційне наповнення сайту може здійснюватися непрофесіоналом, оскільки цей процес не вимагає спеціальної підготовки. Маючи певні навички користування комп'ютером не складно розібратися з системою управління сайтом. Використовуючи простий і логічний інтерфейс і зручні редактори, можна створювати текстове наповнення для сайтів, додавати зображення, мультимедіа, новини, тобто створювати і розвивати самостійно свій проект. Найголовніше, при редагуванні контенту, немає необхідності писати HTML-код, програма сама потурбується про це.

Сайт, що працює на CMS, відрізняється від звичайного сайту тим, що він є динамічним. Подібного роду сайти не лише легко наповнюються контентом і міняють свій дизайн, вони здатні оперативно реагувати на запити користувачів, вкладаючи в готовий шаблон необхідне для користувачів наповнення. Таким чином, завдяки CMS, з'явилася можливість створювати інтернет-магазини, інтернет-ігри, інтернет-співтовариства, системи електронних платежів і інші сервіси, без яких ми вже не представляємо сучасний Інтернет

У загальному випадку системи управління вмістом діляться на: системи управління вмістом масштабу підприємства (англ. Enterprise Content Management System) і системи управління веб-вмістом (англ. Web Content Management System).

− Web content management systems для управління веб-сайтами (наприклад, енциклопедіями, подібними до Вікіпедії, онлайн-виданнями, блогами, форумами, корпоративними або персональними веб-сторінками та ін.);

− Транзакційні CMS для забезпечення транзакцій в електронній комерції;

− Інтегровані CMS для роботи з документацією на підприємствах;

− Електронні бібліотеки (Digital Asset Management) для забезпечення циклу життя файлів електронних медіа (відео, графічні., презентації і тому подібне);

− Системи для забезпечення циклу життя документації (інструкції, довідники, описи);

− Освітні CMS - системи для організації Інтернет курсів і відповідного циклу життя документації;

− Платформені CMS (Platform Content Management Systems) підтримують автоматизацію роботу з комп'ютерними файлами, теками, програмами в певному програмному середовищі;

− Корпоративні CMS (Enterprise content management systems) з різноплановим пристосуванням для потреб підприємницької діяльності. Підтримують цикл життя внутрішньої і зовнішньої документації (RedDot, Rhythmyx, Microsoft CMS, Documentum, Open pages, Blue Martini, Viagnette, Chrystal Software) [1].

Систем управління сайтом існує дуже багато, і всі вони мають свої певні можливості, які краще підходять для вирішення конкретних завдань. Також існують і такі системи, які можна назвати більш-менш універсальними і які підходять для використання на багатьох сайтах. За своїм складом CMS теж бувають різними - якісь системи складаються з безлічі блоків, інші мають неподільну архітектуру. Так само як і інші види програмного забезпечення, CMS можуть бути платними, а можуть поширюватися безкоштовно [3].

Складові CMS:

1. Сховище інформації.

Центральним елементом CMS є сховища інформації. У сучасних системах управління контентом - це реляційна база даних. Слово "реляційна" вказує на те, що база складається з таблиць, між якими встановлені відношення. Якщо CMS необхідно зберегти певну інформацію, вона записує її в базу даних. Для кожної суті в базі даних відведена окрема таблиця. Наприклад, таблиця, яка зберігає вміст веб-сторінок. У ній, окрім тексту сторінки, зберігається назва матеріалу, дата створення і дані про автора. При запиті йде посилання вже на таблицю користувачів, в якій знаходяться їх логіни, паролі і права. За допомогою встановлення спеціальних модулів можна побудувати досить гнучку і надійну систему зберігання інформації. Програмний движок бази даних вибирається залежно від платформи. Якщо використовується платформа Windows, то це MS SQL, якщо UNIX платформа, то MySQL. Після вибору бази даних варто визначитися, як краще

запрограмувати роботу з нею в CMS. Кращим підходом є створення абстрактного прошарку роботи з базою даних. Реалізувати його можна як у вигляді спеціального класу, так і у вигляді набору функцій.

2. Шаблонізатори.

Інформацію, яку необхідно відобразити (наприклад, текст статті), CMS отримує з бази даних. Для відображення інформації у форматі HTML використовується механізм шаблонів. Шаблон - це файл з дизайном сторінки, що створеною засобами спеціальної мови. Зазвичай, це певним чином розмічений код HTML, в якому вказано, де потрібно вставляти назву сторінки, де - основний текст, де - меню або інші елементи, які беруться з бази даних. Простий варіант - створення шаблону мовою PHP.

3. Система користувачів.

Наступною частиною системи є система користувачів і їх ролей. Роль користувача - це певний набір дій, які він може здійснювати. Ролі можна порівняти з групами користувачів в Windows. У сучасних CMS ролі користувача можна створювати і налаштовувати згідно з намірами розробника. Зазвичай, визначають декілька ролей користувачів: адміністратор, модератор, автор, користувач і відвідувач. Кожному користувачеві можна надати певну роль, причому привласнення ролей відбувається або автоматично, або це робиться власноручно адміністратором. Перший варіант часто використовується на форумах, коли після досягнення певної кількості публікацій користувачеві автоматично привласнюється новий статус.

Отже, використання CMS не лише автоматизує і прискорює процес створення сайту, але і значно спрощує його. Фактично з виникненням CMS були зняті технічні обмеження на створення сайту і тепер навіть недосвідченому користувачеві, що не має особливих знань у побудові сайту, під силу створити будь-який тип сайту, будь то сайт-візитка, інформаційний, або сайт-портал [1].

Література:

1. Сучасні інформаційно-комунікаційні технології : навчальний посібник / [Г.Г.Швачич, В.В.Толстой, Л.М.Петречук та ін.] – Дніпро: НМетАУ, 2017. –230 с.

2. Система управління сайтами. Огляд основних CMS. Створення власної системи управління контентом [Електронний ресурс] – Режим доступу : https://works.doklad.ru/view/Bd73uYTDafI.html.

3. CMS [Електронний ресурс] – Режим доступу : https://www.seonews.ru/glossary/cms/.

ХМАРНІ СХОВИЩА ДАНИХ

Андрущенко Катерина Юріївна

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації
м. Київ

Останнім часом у галузі інформаційно-комунікаційних технологій спостерігається бурхливий розвиток хмарних технологій. Відповідно до цього виникають численні хмарні сервіси, що все частіше застосовуються у різних сферах людської діяльності. Їх використовують у науці, освіті, бізнесі тощо. Одним із найпоширеніших подібних сервісів являються хмарні сховища даних, вони мають свої переваги і недоліки, які треба враховувати при прийнятті рішення про їх використання.

Хмарне сховище даних – це модель онлайн сховища, в якому дані зберігаються на численних розподілених у мережі серверах, що надаються в користування клієнтам, в основному, третьою стороною [1]. Завантаживши файли в таке сховище, ви зможете отримати до них доступ з будь-якої точки світу, де є Інтернет [2].

З технічного боку хмарне сховище даних відрізняється від звичайних серверів для зберігання файлів тим, що для зберігання даних використовується величезна кількість серверів. І ваші файли можуть бути розкидані після різних серверів. Але користувача не хвилює внутрішня структура сервісу. Із його точки зору хмара це один великий сервер з яким він і працює. Зараз хмарні сховища даних набирають величезну популярність. Їх використовують не лише комерційні структури, але і приватні користувачі.

Залежно від моделі розгортання хмари бувають:

- private cloud - приватна хмара, призначене для використання однією організацією, може знаходиться як у власності цієї організації, так і якоїсь іншої;
- public cloud - публічна хмара, призначене для вільного використання різними користувачами різних компаній;
- hybrid cloud - гібридна хмара - комбінація з двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних), що залишаються унікальними об'єктами, але пов'язаних між собою стандартизованими або приватними технологіями передачі даних і додатків;
- community cloud - суспільна або комунальна хмара, призначена для використання конкретною спільнотою споживачів з організацій, що мають спільні завдання (наприклад, вимог безпеки). Громадське хмара може перебувати в кооперативній (спільної) власності, управлінні і експлуатації однієї або більше з організацій спільноти або третьої сторони (або будь-якої їх комбінації) [2].

Переваги використання хмарних сховищ:

- доступ до даних здійснюється з будь-якого місця та в будь-який час за наявності під'єднання до глобальної мережі Інтернет;

- користувач сплачує тільки за те місце у сховищі, яке фактично використовує або користується певним обсягом дискового простору хмарного сховища безкоштовно;

- економія дискового простору на жорсткому диску комп'ютера;

- всі процедури із збереження цілісності даних забезпечуються провайдером хмарного центру.

Недоліки використання хмарних сховищ даних:

- небезпека у процесі зберігання та пересилання даних, особливо конфіденційних, приватних;

- загальна продуктивність при роботі з даними в "хмарі" може бути нижчою, ніж при роботі з локальними копіями даних;

- необхідна наявність стабільного та швидкісного під'єднання до мережі Інтернет.

Отже, за останній час хмарні сховища даних набули великої популярності і є частиною нашого повсякденного життя. Хмарні технології інтенсивно розвиваються і надалі будуть ставати зручнішими та універсальними [1].

Література:

1. Хмарні сховища даних та їх характеристики [Електронний ресурс] – Режим доступу : https://informatika.udpu.edu.ua/?page_id=1896.

2. Сучасні інформаційно-комунікаційні технології: навчальний посібник / [Г.Г.Швачич, В.В.Толстой, Л.М.Петречук та ін.] – Дніпро: НМетАУ, 2017. –230 с.

ЗАСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ ПОВ'ЗАНИХ З ЛЮДСЬКИМ ФАКТОРОМ

Ахтьоров Владислав Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Незважаючи на значний вплив людського фактору на інформаційну та кібернетичну безпеку доволі часто йому не приділяють відповідної уваги обмежуючись лише організаційними заходами. Проаналізувавши всі можливі загрози пов'язані з людським фактором можна визначити необхідні сучасні програмно-апаратні засоби для захисту від можливих загроз інформації від умисних та випадкових шкідливих дій внутрішніх користувачів.

Людський фактор можна визначити як можливий вплив людини на стан та функціонування системи. В інформаційній безпеці він грає значну роль, дуже часто залишаючись однією з найуразливіших частин системи захисту інформації. На підприємствах людський фактор представляє собою

співробітників які взаємодіють з автоматизованою системою, тобто є внутрішніми користувачами. Для зниження загрози від користувачів найчастіше приймаються організаційні заходи в вигляді навчання персоналу, формування правил користування АС. Проте на сьогоднішній день існує багато програмно-апаратних засобів які здатні ефективно нейтралізовувати загрозу від людського фактору. Для вибору таких засобів необхідно проаналізувати можливі загрози та на основі цього підібрати відповідне програмне забезпечення, налаштування тощо.

Серед можливих загроз можна виділити випадкові (випадкове нанесення фізичної шкоди робочій станції, порушення правил користуання) та умисні (передача конфіденційних даних конкурентам, умисне занесення шкідливого програмного забезпечення до АС). Дуже часто зловмисники використовують соціальну інженерію для реалізації інформаційної загрози через користувачів. Соціальна інженерія – це використання психологічних навичок впливу для отримання певної інформації, або спідкання користувача до виконання певних дій в автоматизованій системі. До методів соціальної інженерії можна віднести претекстінг, маскування під внутрішнього користувача, конкурентна розвідка [1].

Зважаючи на ці загрози ефективними будуть засоби реєстрації та контролю зйомних носіїв, системи моніторингу діяльності користувачів під час роботи з АС, системи контролю за передачою та модифікацією конфіденційних даних. Сучасним рішенням яке може включати всі наведені вище засоби є DLP-система. DLP-система – це система, яка захищає конфіденційні дані від витоку каналами зв'язку. Дві основні функції : визначення конфіденційних даних різними методами аналізу та моніторинг передачі конфіденційних даних. Дуже часто подібні системи можуть побічно виконувати наведені вище задачі : контроль зйомних носіїв, моніторинг діяльності користувачів тощо. Відповідні параметри задаються через налаштування політик безпеки всередені системи. Можна виділити пасивні та активні види DLP [2]. Активні здатні самостійно блокувати дії, які порушують задану політику , в той час як пасивні лише створюють звіти або відправляють відповідні попередження про порушення політики безпеки.

Зазвичай всі наведені вище рішення (від окремих систем моніторингу до DLP) мають клієнт-серверну архітектуру[3]. Клієнти встановлюються на робочих станціях користувачів та виконують відповідну політику безпеки задану сервером. Всі налаштування проводяться в відповідній консолі. Такий підхід дозволяє оперативно реагувати на інцеденти, проводити їх

розслідування. Також можлива інтеграція з іншими системами безпеки, такими як SIEM, що дозволяє доповнювати вже існуючу систему безпеки вже існуючу на підприємстві.

Розширивши систему додавши захист конфіденційних даних та контроль за діяльністю внутрішніх користувачів можна значно підвищити рівень інформаційної безпеки. З врахуванням людського фактору в системі захисту у зловмисників буде значно менше можливостей реалізувати інформаційні загрози на АС підприємства.

Література:

1. Красовська Є. В. ПРОГРАМНИЙ КОМПЛЕКС МОНІТОРИНГУ АКТИВНОСТІ КОРИСТУВАЧІВКОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖ / Є. В. Красовська. // Електротехнічні та комп'ютерні системи. – 2012. – С. 85–92.

2. Корпоративная безопасность: что такое DLP-система и зачем она нужна бизнесу [Електронний ресурс] // Control Engineering Россия Апрель 2017. – 2017. – Режим доступу до ресурсу: https://www.controlengrussia.com/programmnye-sredstva/bezopasnost-programmnye-sredstva/data-leak-prevention/.

3. Мельниченко О. В. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ ПРИ РОБОТІ З ЕЛЕКТРОННИМИ ГРОШИМА / О. В. Мельниченко. // Проблеми економіки. – 2013. – №4. – С. 341–347.

ДОСЛІДЖЕННЯ АСПЕКТІВ БЕЗПЕКИ ВЕБ СЕРВІСІВ

Баргилевич Олександр Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Кожен день ми користуємося Web-сайтами для різних потреб, таких як: спілкування с друзями, рідними; навчання; оплата комунальних послуг або придбання необхідних речей. З зростанням попиту на сайти зростає необхідність їх захисту. В досліджуваній статті надано методи та реалізації задля запобігання порушення доступності, цілісності та конфіденційності веб сервісу. Даний матеріал буде цікавим розробникам, менеджерам, спеціалістам з оцінки якості.

Метою проекту «OWASP Pro Active Control» є привернення уваги до безпеки сайтів та сервісів, шляхом розгляду найбільш важливих аспектів безпеки, на які розробникам варто звертати увагу. Однією з основних цілей даної статті є створення практичного керівництва, що дозволяє створювати безпечне програмне забезпечення. В статті надається рейтинг з 10 вимог до захисту.

C1: Визначення вимог безпеки - описують функції, які необхідно реалізувати для забезпечення певних параметрів безпеки веб сервісів. Вони складаються на основі стандартів, чинних законів і даних про виявлені вразливості. Процес успішного застосування вимог безпеки включає в себе чотири етапи: пошук і вибір, документування, реалізація,

підтвердження правильності реалізації нових функцій безпеки і функціональності додатку.

C2: Використання безпечних фреймворків і бібліотек – використання розробниками бібліотек що користуються популярністю та мають підтримку компаніями, що мінімізує потрапляння злоякісного коду.

C3: Забезпечення безпечного доступу до баз даних – цей розділ посвячується безпечному доступу до баз даних та поєднує 4 розділи: безпека запитів, конфігурації, аутентифікації, з'єднань.

C4: Кодування та захист даних - є методами захисту від впровадження коду. В контексті кодування мається на увазі перетворення символів в еквівалентні, задля забезпечення відповідності та безпеки. В контексті екранування мається на увазі мутація символів для відображення.

C5: Обов'язкова перевірка всіх вхідних даних - перевірка вхідних даних є частиною методики програмування, забезпечує потрапляння в компоненти програми тільки правильно відформатованих даних.

C6: Впровадження цифрового ідентифікації - це унікальне уявлення користувача (або будь-якого іншого об'єкта) при онлайн-транзакціях. По суті процес, за допомогою якого сервер контролює стан аутентифікації користувача.

C7: Обов'язковий контроль доступу - полягає в дозволі або забороні специфічних запитів, що надходять від користувачів, програм або процесів, а також передбачає видачу та відкликання подібних привілеїв.

Існує кілька різних підходів до контролю доступу:

- виборче управління доступом (DAC)
- мандатний управління доступом (MAC)
- рольова модель управління доступом (RBAC)
- управління доступом на основі атрибутів (ABAC)

C8: Повсюдний захист даних – процес посиленого захисту чутливої інформації. Конфіденційні дані, такі як паролі, номери кредитних карт, вимагають додаткового захисту, особливо якщо вони підпадають під дію закону про недоторканність даних.

C9: Впровадження журналювання та моніторингу подій безпеки - важливо реєструвати події безпеки (дані, пов'язані з забезпеченням безпеки) під час роботи програми. В даному контексті моніторинг - це одночасний аналіз програми та журналів безпеки за допомогою різних засобів автоматизації.

C10: Обов'язкова обробка всіх помилок і виключень - дозволяє додатку реагувати на різні різними способами.

Коректна обробка виключень і помилок просто необхідна для забезпечення надійності і безпеки коду.

Література:

1. OWASP Top 10 Proactive Controls [Електронний ресурс] – Режим доступу: https://github.com/OWASP/www-project-proactive-controls/blob/master/v3/OWASP_Top_10_Proactive_Controls_V3.pdf

БОТНЕТ - НАЙБІЛЬША ЗАГРОЗА В ІНТЕРНЕТІ?

Бугай Олексій Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Що таке ботнет, і як дізнатися, що ваш комп'ютер «зомбі»?
Ваш комп'ютер поводиться підозріло?
Упала потужність, занадто великі рахунки за інтернет-трафік?
Часом гальмує інтернет і підвисає комп'ютер?
Можливо вся справа в тому, що ваш ПК став частиною ботнету.

Слово ботнет походить від англійських слів «robot» (робот) і «network» (мережа). По суті, це - мережа комп'ютерів, що заражена шкідливим програмним забезпеченням, які управляються зловмисниками з командного центру.

Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних шкідливих дій без відома користувачів.

За допомогою ботнетів часто передається спам, встановлюються шпигунські програми або здійснюється крадіжка облікових даних користувачів.

Масштабний ботнет може використовуватися для атак типу DDoS (Distributed Denial of Service) для направлення додаткового трафіку на сайт і уповільнення роботи ресурсу або збоїв підключення. Шкідливі програми виду ботнет поширюються за допомогою вкладень електронної пошти і через завантаження файлів і підроблених програм.

Ці шкідливі програми працюють непомітно, використовуючи при цьому системні ресурси комп'ютера користувача. І найчастіше користувач навіть не здогадується, що його комп'ютер «зомбі». Основні можливості ботнетів Перехоплення даних, які користувач вводить (логіни, паролі, дані кредитних карт) і передача їх в командний центр Атаки на конкретні інтернет-ресурси. Зловмисники також націлюються на такі вразливі місця, що не оновлене програмне забезпечення та відсутність захисту в мережі Інтернет. Все частіше під приціл

зловмисників потрапляють камери, смарт-телевізори і навіть автомобілі.

Після зараження комп'ютер стає частиною бот-мережі - мережі інфікованих комп'ютерів, керованих на відстані кіберзлочинцем, який орендував її для здійснення незаконних планів. Таким чином, не лише компрометується ваша інтернет-безпека, але й ваші системні ресурси і пропускна здатність здаються в оренду, щоб допомогти напасти на інших користувачів або організації. Цей величезний потенціал для кіберзлочинності робить бот-мережі однією з найбільш небезпечних загроз в Інтернеті, на думку деяких експертів.

Бот-мережі складаються з сотень або тисяч інфікованих пристроїв та мають ресурси, необхідні для виконання таких шкідливих дій, як доставка масових спам-повідомлень, DoS і DDoS-атаки, атаки шляхом масового зламу паролів, крадіжка акаунтів та інтернет-шахрайство шляхом збору особистої інформації від інфікованих користувачів.

Більше 80% світового спаму розсилається з зомбі-комп'ютерів. Недобросовісна спам-реклама, атаки на певні ресурси, крадіжка банківських рахунків користувачів або просто продаж або здача в оренду ботнету дозволяє своєму власникові заробляти хороші гроші. Так що кіберзлочинці зацікавлені в зараженні якомога більшої кількості комп'ютерів і поширенні ботнетів. Тому нерідко в спамі, який розсилають, містяться шкідливі файли, що вражають не заражені ПК.

Чому потрібно використовувати захист від ботнетів?

Якщо Ваш комп'ютер став частиною ботнет-мережі, це може негативно впливати на роботу комп'ютера.

Обчислювальна потужність одного ботнету дозволяє здійснювати шкідливі дії швидко і часто без виявлення. Наприклад, в 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка викликала збої в роботі таких сайтів як Twitter, Amazon і Netflix.

Щоб не стати частиною ботнету, важливо дотримуватися таких правил безпеки.

- Виконуйте регулярне оновлення програмного забезпечення і виправлення помилок.

- Використовуйте рішення для забезпечення безпеки в Інтернеті з захистом від ботнет-атак . Такі рішення виявляють і блокують загрози і використовують брандмауер для фільтрації зв'язку між комп'ютером та Інтернетом.

- Будьте обережні, завантажуючи файли або програми і відкриваючи вкладення.

Як захистити свій комп'ютер

Зловмисники включають комп'ютери в ботнети за допомогою двох основних стратегій: Вони спробують спонукати користувача встановити їх шкідливе програмне забезпечення. Встановлення зловмисного програмного забезпечення через уразливими деяких програм або через злам облікових записів, які захищаються ненадійними паролями.

Перше, що потрібно зробити, щоб захистити комп'ютер від «зомбування» — це встановити антивірусну програму. Варто подбати про регулярне оновлення програмного забезпечення на комп'ютері.

Також потрібно використовувати надійні паролі і зберігати їх у безпечному місці (наприклад, в менеджері паролів). Не варто відключати брандмауер. Брандмауер створює захисний заслін між вашим комп'ютером та Інтернетом. Вимкнення брандмауера навіть на хвилину збільшує ризик зараження ПК шкідливою програмою. Зараження «зомбі-вірусом» проблема, яка стосується кожного. Масштаб цієї загрози неймовірно великий, за оцінками експертів, чверть всіх комп'ютерів підключених до Інтернету можуть перебувати в ботнет. Тому потрібно починати думати про безпеку свого ПК вже зараз.

Література:

1.https://rmrf.tech/uk_UA/blog/rmrf-1/post/17

2.https://zillya.ua/shcho-take-botnet-i-yak-diznatisya-shcho-vash-kompyuter-%C2%ABzombi%C2%BB

3.https://eset.ua/ru/support/entsiklopediya_ugroz/zashchita_ot_botnetov

АНАТОМІЯ DoS АТАКИ

Вакуленко Ольга Сергіївна

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації

м. Київ

Експлуатуючи особливості, властиві TCP протоколу, віддалені нападники можуть ініціювати DoS на широкий масив операційних систем.

DoS-атака (від англ. Denial of Service – «відмова в обслуговуванні») – атака, яка використовується для виведення з ладу і злому обчислювальної техніки і створення технічних і економічних труднощів у мети. Здійснюється за допомогою створення великої кількості запитів і серйозного навантаження на техніку, найчастіше на великі сервера.

Напад найбільш ефективен проти HTTP серверів. Наданий сценарій Perl демонструє цю проблему.

При TCP зв'язку, кожна TCP розподіляє деякі ресурси кожному підключенню. Неодноразово встановлюючи TCP підключення і потім, відмовляючись від них, зловмисний хост може пов'язувати істотні ресурси на сервері. Сервер Unix може виділяти певний номер mbufs або навіть процес на кожне з таких підключень. Пройде деякий час перш, ніж частина ресурсів буде повернута до системи. Якщо створити багато невиконаних залишених підключень такого виду, система може руйнуватися або просто припиняти обслуговувати специфічний порт.

Будь-яка система, яка виконує TCP службу, може бути атакована цим шляхом. Ефективність такого нападу залежить від дуже великої кількості факторів. Web сервери особливо уразливі до такого нападу через природи протоколу (короткий запит генерує довільно довгий відповідь).

Уразливість може бути використана проти різних сервісів. Тут буде обговорено, як її використовувати проти HTTP серверів. Механізм досить простий: Після інструктування нашого ядра, щоб не відповідати на будь-які пакети від цільової машини (найбільш легко зробити з використанням систем захисту мереж, поле: з ipfw, "deny any from TARGET to any"), неодноразово инициализируем нове підключення від випадкового порту , посилаючи SYN пакет, чекаючи SYN + ACK відповідь, і потім посилаючи наш запит (можна було б більш традиційно спочатку підтверджувати SYN + ACK і тільки потім посилати запит, але це шлях, який економить пакети. Напад є більш ефективним, коли цим шляхом обраний статичний файл, а не динамічний зміст. Природа файлу не має значення (графіка, текстовий або просто HTML) але розмір має велику важливістю. Що почне робити сервер, коли він отримує ці підроблені запити? Перш за все, ядро обробляє встановлення TCPсвязі; оскільки ми посилаємо наш другий пакет, і встановлення зв'язку таким чином закінчено, користувальницький додаток повідомлено про запит (повернення системного виклику введення, підключення тепер встановлено). У той час, ядро має дані запиту в отриманні черзі. Процес читає запит (який є HTTP / 1.0 без будь-якої діючої опції), інтерпретує його, і потім записує деякі дані в дескриптор файлу і закриває його (підключення входить в стан FIN_WAIT_1). Процес тоді використовує певний з'їдений mbufs, якщо ми досягаємо цього пункту.

Цей напад містить два різновиди: mbufs виснаження і насиченість процесу. При виконанні mbufs виснаження, каждрое підключення використовує процес користувацького рівня на іншому кінці, для запису даних без блокування і закриття дескриптора. Ядро має мати справу з усіма даними, і процес

користувацького рівня буде звільнений, так, щоб ми могли посилати більшу кількість запитів цим шляхом і в кінцевому рахунку споживати весь mbufs або всю фізичну пам'ять, якщо mbufs розподілений динамічно.

При виконанні насиченості процесу, кожен хоче, щоб процес користувацького рівня блокувався при спробі записати дані. Архітектура багатьох HTTP серверів дозволяє обслуговувати багато підключень одночасно. Коли ми досягаємо цього числа підключень, сервер припинить відповідати законним користувачам. Якщо сервер не поміщає зв'язку на числі підключень, ми все ще пов'язуємо ресурси і, в кінцевому рахунку, система приходить до краху. Mbufs виснаження зазвичай не має ніякого видимого ефекту поки ми не досягаємо жорсткого межі номера кластерів mbuf або mbufs. У цій точці, формується дамп kernel core, перезавантаження, перевірка файлової системи, відновлення дампа ядра – все це забирають багато часу операції. Все це прекрасно працює з FreeBSD та інших BSD заснованих платформах. Деякі інші системи, типу Linux, здається, розподіляють довільний обсяг пам'яті для кластерів mbuf. Як тільки ми наближаємося до фізичному обсягу пам'яті, машина стає повністю непридатною.

Якщо у вас стався збій сервісу, такі ознаки допоможуть ідентифікувати цей інструмент:

- Ваші HTTP сервери мають сотні або тисячі підключень з 80 портом в стані FIN_WAIT_1.
- Коефіцієнт (число йдуть пакетів / номери вхідних пакетів) незвично високий.
- Є велика кількість підключень з 80 портом у встановленому стані, і більшість їх має однакову довжину. (Або, є великі групи підключень, спільно використовують те ж саме нульове значення довжини).

Література:

1. SecurityLab. Универсальное удаленное нападение DoS / Режим доступу: [https://www.securitylab.ru/analytics/216177.php]

2. Контел. Как защитить ЦОД от DDoS-атак? / Режим доступу: [https://habr.com/ru/company/contell/blog/332406]

THREATS, RISKS AND VULNERABILITIES IN CYBERSECURITY. SUMMARY

Vereta Anton Oleksandrovych
State University of Telecommunications
Institute of Cybersecurity

What do we mean by cybersecurity? Cybersecurity is a method, process and technology designed to protect programs, networks and, most importantly, our data. Data is an asset. In today's world, information has the greatest value and significance, and the weakest point in its protection is the people themselves. Any organization (government or commercial structures, finance or medicine) accumulates, stores, operates a large amount of data of users, customers, employees and more.
Keywords: ITU-T, cybersecurity, confidential data.

In general terms, there is a need to protect assets for:

• customers/subscribers who need confidence in the network and the services offered, including availability of services (especially emergency services);

• public community/authorities who demand security by directives and/or legislation, in order to ensure availability of services, privacy protection, and fair competition; and

• network operators and service providers who need security to safeguard their operation and business interests and to meet their obligations to customers, their business partners and the public. The assets to be protected include:

• communication and computing services;

• information and data, including software and data relating to security services;

• personnel; and

• equipment and facilities.

A security threat is defined as a potential violation of security. Examples of threats include:

• unauthorized disclosure of information;

• unauthorized destruction or modification of data, equipment or other resources;

• theft, removal or loss of information or other resources;

• interruption or denial of services; and

• impersonation, or masquerading as an authorized entity.

Threats may be accidental (also sometimes called inadvertent) or intentional and may be active or passive. An accidental threat is one with no premeditated intent such as a system or software malfunction or a physical failure. An intentional threat is one that is realized by someone committing a deliberate act. Intentional threats may range from casual examination, using easily-available monitoring tools, to sophisticated attacks using special system knowledge. When an intentional threat is realized it is called an attack. An active threat is one that results in some change to the state or operation of a system, such as alteration of data or destruction of physical equipment. A passive threat involves no change of state. Eavesdropping and wiretapping are examples of passive threats.

A security vulnerability is a flaw or weakness that could be exploited to violate a system or the information it contains. If a vulnerability exists, then it is possible for a threat to be realized successfully unless effective countermeasures are in place. ITU-T Recommendations recognize four types of vulnerability:

• threat model vulnerabilities, which result from failure to foresee possible future threats;

• design and specification vulnerabilities, which result from errors or oversights in the design of a system or protocol and make it inherently vulnerable;

• implementation vulnerabilities, which are introduced by errors or oversights during system or protocol implementation; and

• operation and configuration vulnerabilities, which originate from improper usage of options in implementations or weak deployment policies and practices (such as failure to use encryption in a wireless network).

Security risk is a measure of the adverse effects that can result if a security vulnerability is exploited, i.e., if a threat is realized. While risk can never be eliminated, one objective of security is to reduce risk to an acceptable level. In order to do that, it is necessary to understand the applicable threats and vulnerabilities and to apply appropriate countermeasures. These are usually specific security services and mechanisms which may be complemented by non-technical measures such as physical and personnel security. While threats and threat agents change, security vulnerabilities exist throughout the life of a system or protocol, unless specific steps are taken to address them. With standardized protocols being very widely-used, vulnerabilities associated with the protocols can have very serious implications and be global in scale. Hence, it is particularly important to understand and identify vulnerabilities in protocols and to take steps to eliminate them as and when they are identified. Standards bodies have both a responsibility and a unique ability to address security vulnerabilities that may be inherent in specifications such as architectures, frameworks and protocols. Even with adequate knowledge about the threats, risks and vulnerabilities associated with information processing and communications networks, adequate security cannot be achieved unless security measures are systematically applied in accordance with relevant security policies. The security policies themselves must be reviewed and updated periodically. Also, adequate provision must be made for security management and incident response. This will include assigning responsibility and specifying action that must be taken to prevent, detect, investigate and respond to any security incident.

Security services and mechanisms can protect telecommunication networks against malicious attacks such as denial of service, eavesdropping, spoofing, tampering with messages (modification, delay, deletion, insertion, replay, re-routing, misrouting, or re-ordering of messages), repudiation or forgery. Protection techniques include prevention, detection and recovery from attacks, as well as management of security-related information. Protection must include measures to prevent service outages due to natural events (such as storms and earthquakes) and malicious attacks (deliberate or violent actions). Provisions must also be made to facilitate interception and monitoring by duly-authorized legal authorities.

Telecommunication network security also demands extensive cooperation between service providers.

Recommendation ITU-T E.408 provides an overview of security requirements and a framework that identifies security threats to telecommunication networks in general (both fixed and mobile; voice and data) and gives guidance for planning countermeasures that can be taken to mitigate the risks arising from the threats.

Implementing the requirements of ITU-T E.408 would facilitate international cooperation in the following

areas relating to telecommunication network security:

• information sharing and dissemination;
• incident coordination and crisis response;
• recruitment and training of security professionals;
• law enforcement coordination;
• protection of critical infrastructure and critical services; and
• development of appropriate legislation.

However, to succeed in obtaining such cooperation, implementation of the requirements for the national components of the network is essential. Recommendation ITU-T X.1205 provides a taxonomy of security threats from an organizational point of view along with a discussion of the threats at the various layers of a network.

Література:

1. Прокоф'єв І.В. Введення в теоретичні основи комп'ютерної безпеки: навчальний посібник / І.В. Прокоф'єв - М.: МІФІ, 2008. - 287 с.

2. Звіт ФБР // Business email compromise the $26 billion scam // вересень 10, 2019. URL: https://www.ic3.gov/media/2019/190910.aspx

3. Д. Акерлоф, Р. Шиллер. Фішинг: Хто і як маніпулює вашим вибором / пер. з англ. О. Герасимчук. – К.: Наш формат, 2017. – 272 с.

4. Митник К.Д. Мистецтво обману: метод. посібник / К.Д. Митник - NYC: Wiley Books. 2008 - 273 с.

ЗАСТОСУВАННЯ GRID-ТЕХНОЛОГІЇ В МЕДИЦИНІ

Вовк Надія Ігорівна
Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації
м. Київ

GRID - технології останнім часом набувають все більшого розвитку та впровадження в науці, економіці, медицині, освіті. В світі створено кілька потужних координаційних центрів щодо їх застосування. В медицині виконується ряд проектів, що потребують великих обчислювальних ресурсів: розшифровка генома, віртуальні госпіталі, пошуки нових ліків, дослідження з епідеміології.

Формування структур інформаційного суспільства є сьогодні одним із пріоритетів нашої держави. Широке застосування новітніх технологій у всіх сферах життєдіяльності суспільства, особливо в медицині, потребує залучення потужних комп'ютерних і обчислювальних ресурсів, у тому числі у сфері збереження та оброблення експериментальних даних.

Грід, термін в дослівному перекладі з англійської означає «ґрати», «сітка», утворюється власниками обчислювальних ресурсів як середовище колективного комп'ютингу, яке вони надають у спільне використання. Таке розподілене об'єднання комп'ютерних ресурсів фактично віртуально генерує створення потужного гіперкомп'ютера. Зростання швидкості обчислень та ефективності використання ресурсів досягається за рахунок того, що виконання обчислювальної задачі можна розпаралелити на велику кількість вільних процесорів, оскільки відомо, що комп'ютери протягом доби більшу частину часу простоюють і в середньому завантажені на 5-10 відсотків. Ця ж проблема також актуальна для великих обчислювальних центрів. Необхідність такого об'єднання обчислювальних ресурсів та ліній зв'язку обумовлена вимогами щодо створення все більш потужних обчислювальних ресурсів для розв'язання особливо складних задач. Одночасно мінімізуються витрати на підтримку працездатності обладнання та його модернізацію.

Грід-технології відразу ж знайшли широке застосування в науці, медицині, освіті, бізнесі. За темпами розвитку грід-технології в останнє десятиріччя значно випереджають Інтернет. Одночасно вони дозволяють доповнити Всесвітню мережу можливостями доступу до обчислювальних ресурсів і створюють систему, яку умовно називають обчислювальним Інтернетом, хоча слід зауважити, що грід-технології — це не тільки обчислення. З'явився навіть новий термін «World Wide Grid — WWG», і в цьому сенсі грід-технології розглядають як еволюційне продовження Інтернету.

Зрозуміло, що робота з медичною інформацією має свої особливості. Історично першим прикладом упровадження грід-технологій для інформаційного супроводу медичних досліджень був проект MAMMOGRID (дослідження раку молочної залози.

Його розпочато у 2002 році для архівування досліджень молочної залози на базі двох британських і одного італійського госпіталю.

Відділ електронної медицини при Європейській комісії визначив кілька причин, які стимулюють упровадження грід-технологій:

• поліпшення якості обслуговування завдяки швидкій діагностиці, своєчасному лікуванню та мінімізації медичних помилок;

• зниження собівартості проведення діагностичних обстежень;

• зниження вартості лікування завдяки ранньому виявленню патологій і вибору оптимальної стратегії лікування.

Ще одним важливим сектором медицини, де використовують переважно обчислювальні потужності грід-технологій, є медичні дослідження геному людини, з пошуку нових ліків, моделювання біомедичних систем. Застосування грід-технологій у медичних дослідженнях залежить значною мірою від наявності комп'ютерних ресурсів, можливостей роботи з великими базами даних та розв'язування надскладних завдань. Яскравим прикладом ефективності грід-технологій є дослідження вірусу пташиного грипу H5N1, яке виконували в проекті WISDOM.

Ще одним напрямом застосування грід-технологій є моделювання «віртуальної» людини. Біомедичні моделі мають багато внутрішніх взаємозв'язків, їхня еволюція пов'язана з перебігом складних фізичних і хімічних процесів, тому для моделювання таких систем необхідні великі обчислювальні ресурси та інтенсивні обрахунки. Моделювання «віртуальної» людини можна здійснити тільки при наявності дуже великих обчислювальних ресурсів.

Література:

1. В. Авраменко, А. Загородній, Є. Мартинов – Особливості застосування грід-технології в медицині // Вісник НАН України. - 2018. -№ 6

2. В.І.Авраменко, І.В.Романенко – Деякі аспекти застосування грід-технологій в медицині // Український журнал телемедицини а медичної телематики. – 2019.

ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ

Вовк Надія Ігорівна

Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації

м. Київ

Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу коштів на всіх етапах її формування, обробки, передачі та зберігання.

Інформаційна безпека означає можливість протистояти спробам нанесення збитків власникам або користувачам платіжної системи при різних навмисних або ненавмисних впливах на неї. Електронні документи, що містять інформацію, яка належить до банківської таємниці або є конфіденційною, повинні бути зашифрованими під час передавання їх за допомогою телекомунікаційних каналів зв'язку.

В науковій літературі відсутнє чітке визначення безпеки платіжної системи. Більшість авторів розглядає безпеку платіжної системи з точки зору її інформаційної складової. Проте, як зазначається в науковій літературі, основними елементами сучасної платіжної системи є:

– нормативно-правова база, що регулює платіжні відносини, має створювати сприятливі умови для забезпечення потреб нормального функціонування платіжної системи;

– бухгалтерська і технологічна модель, що є основним операційним механізмом здійснення платежів, що ґрунтується на принципах бухгалтерського обліку і звітності, включає платіжні інструменти та механізми переказу коштів;

– технологічна інфраструктура, що є основою життєздатності платіжної системи; вона включає, зокрема, програмні та технічні засоби обробки та передачі даних, обслуговуючий персонал;

– захист інформації як сукупність програмно-технічних, нормативно-правових, адміністративно-організаційних засобів.

Тобто стає зрозумілим, що інформаційна безпека є останнім елементом платіжної системи, а тому для забезпечення її ефективного функціонування потрібно всі елементи розглядати у системній єдності і тісному взаємозв’язку.

Безпеку платіжних систем можна розглядати як таку, що складається зі зовнішньої та внутрішньої.

Зовнішня безпека включає:

- захист від втрати або модифікації системою інформації при стихійних лихах (пожежах, землетрусах та ін.);

- захист системи від проникнення зловмисників ззовні з метою викрадення, отримання доступу до інформації або виведення системи з ладу [1].

Мета внутрішньої безпеки — забезпечення надійної та коректної роботи, цілісності інформації і компонентів (ресурсів) системи. Це передбачає створення надійних і зручних механізмів регламентування діяльності всіх користувачів та

обслуговуючого персоналу, підтримання дисципліни доступу до ресурсів системи.

Можна виділити два підходи до гарантування безпеки інформаційних систем: фрагментарний та комплексний.

Фрагментарний підхід орієнтується на протидію чітко визначеним загрозам при певних умовах використання системи. Головною позитивною рисою такого підходу є міцний захист щодо конкретної загрози, але основний недолік — локальність дії та відсутність єдиного захищеного середовища для обробки інформації. Тому такий підхід неприйнятний для захисту платіжних систем [2].

Для створення захисту платіжних систем треба використовувати комплексний підхід, а саме: створення захищеного середовища для обробки платіжної та службової інформації в системі, яке об'єднує різноманітні (правові, організаційні, програмно-технічні) засоби для протидії будь-яким загрозам.

Література:

1. Платіжні системи : [навч. пос.] / [О. Вовчак, Г. Шпаргало, Т. Андрейків]. – К. : Знання, 2008. – с.341

2. ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ [Електронний ресурс]. – Режим доступу: https://pidru4niki.com/10810806/finansi/zahodi_zahistu_informatsiynoyi_bezpeki_platizhnih_sistem

СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ПРО БЕЗПЕКУ ТА УПРАВЛІННЯ ПОДІЯМИ

Вовк Надія Ігорівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Оскільки практично більшість підприємств працюють в Інтернеті, все важливіше використовувати інструменти кібербезпеки та виявлення загроз для запобігання простоїв роботи. На жаль, у мережі багато активних недобросовісних зловмисників, які лише чекають удару по вразливих системах. Інформація про безпеку та управління подіями (SIEM) стали основною частиною виявлення та подолання кібератак.

Розвиток інформаційних технологій спрощує ведення бізнесу. Однак, чим більше джерел даних з'являється в корпоративних IT-системах, тим складніше стають завдання адміністраторів інформаційної безпеки, які не встигають «вручну» відстежувати і блокувати загрози. Без своєчасного моніторингу та запобігання несанкціонованих дій втрачається сенс системи захисту інформації. І тут на допомогу ІБ-фахівцям

приходять рішення класу SIEM - Security Information and Event Management [1].

Сучасні кіберзлочинці не атакують безпосередньо IT-інфрастуктуру. Вони діють завуальовано, використовуючи вразливості захисних ресурсів. Такі інциденти залишаються поза увагою, так як без «контексту» не вказують на загрозу. Відстежити протиправні дії допомагає постійний моніторинг і аналіз всіх подій, що відбуваються в IT-інфраструктурі компанії. Таку здатність аналізувати і виявляти інциденти по окремим подіям мають SIEM-рішення [1].

Системи захисту, відомі під абревіатурою SIEM, з'явилися в результаті еволюції і злиття SEM і SIM.

SEM – Security Event Management – система захисту, яка працює в режимі реального часу. Вона самостійно спостерігає за подіями в інформаційних потоках, збирає їх, виробляє кореляцію і генерує превентивні повідомлення.

SIM – Security Information Management – система, яка відповідає за аналіз відомостей на основі статистики та девіацій від встановлених правил безпеки.

Абревіатура SIEM означає «Система Збору та Кореляції Подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому – аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів і призначених для користувача ПК, і при цьому детектувати відхилення від норм по якимось критеріям. Якщо таке відхилення виявлено – система генерує інцидент. Варто відзначити, що в основі роботи SIEM лежать, в основному, статистичні та математичні технології, схожі на ті, що використовуються, наприклад, в BI-системах.

Для виконання свого завдання сучасні SIEM-системи використовують такі джерела інформації:

- Access Control, Authentication. Застосовуються для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- DLP-системи. Відомості про спроби інсайдерських витоків, порушення прав доступу.
- IDS / IPS-системи. Несуть дані про мережеві атаки, зміни конфігурації і доступу до пристроїв.
- Антивірусні програми. Генерують події про працездатність ПО, базах даних, зміні конфігурацій і політик, шкідливий код.

- Журнали подій серверів і робочих станцій. Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- Міжмережеві екрани. Відомості про атаки, шкідливі програми та інше.
- Мережеве активне обладнання. Використовується для контролю доступу, обліку мережевого трафіку.
- Сканери вразливостей. Дані про інвентаризацію активів, сервісів, ПО, вразливостей, поставка інвентаризаційних даних і топологічної структури.
- Системи інвентаризації та asset-management. Поставляють дані для контролю активів в інфраструктурі і виявлення нових [2].
- Системи веб-фільтрації. Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів.

Отже, основні завдання SIEM-систем такі:

1. Отримання журналів з різноманітних засобів захисту;
2. Нормалізація отриманих даних;
3. Таксономія нормалізованих даних;
4. Кореляція класифікованих подій;
5. Створення інциденту, надання інструментів для проведення розслідування;
6. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців);
7. Швидкий пошук по SIEM даним, що зберігаються [3].

Крім зазначеного функціоналу, SIEM-системи можуть також оснащуватися додатковими функціями, такими як управління ризиками та уразливими, інвентаризація IT-активів, побудова звітів і діаграм і т.д.

Література:

1. ЧОМУ ВАЖЛИВЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ?: [Електронний ресурс]. – Режим доступу: https://softlist.ua/rishennia/rishennia-z-informatsiinoi-bezpeky/siem

2. SIEM (Security information and event management) .- [Электронный ресурс].- Режим доступа: https://ru.bmstu.wiki/SIEM_(Security_information_and_event_managemen)

3. SIEM системы - что это такое и зачем нужно? .- [Электронный ресурс].- Режим доступа: https://www.securityvision.ru/blog/siem-chto-eto-i-zachem-nuzhno/

ОСОБЛИВОСТІ МОНІТОРИНГУ ВЕБ-СЕРВІСІВ ЗА ДОПОМОГОЮ ELK STACK

Гаврилей Олександр Петрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Масштаб, склад і структура кіберзагроз для організацій швидко еволюціонують. Будь-який бізнес потребує впровадження систем для моніторингу IT-інфраструктури та швидкого реагування на інциденти, щоб забезпечити запуск і подальшу роботу необхідних йому мережевих систем і сервісів. Однак здійснення моніторингу різних складових частин IT-інфраструктури може стати для організації складним етапом, якщо заздалегідь не було сплановано для цих цілей. Незалежно від масштабів інфраструктури, будь вона невеликого розміру або рівня підприємства, в будь-якому випадку організація не може обійтися без надійного інструментарію для моніторингу та реагування на інциденти.

Сучасні порушники постійно намагаються вдосконалювати свої методи та інструменти задля успішного проведення кібератак. А стрімке збільшення інформаційного потоку змушує організації розглядати нові варіанти захисту критичної інформації, забезпечуючи стабільність та захищеність інформаційної системи яку щороку стає все складніше захищати.

Для створення захищеної інфраструктури, спеціалістам потрібно слідкувати за величезною кількістю подій які відбуваються в системі. Для покращення процесів моніторингу за подіями та превентивного підходу до дій порушників, компанія Elastic розробила ряд рішень під назвою ELK Stack, які надають змогу поєднати інструменти для інтегрування інформації про захищеність, події та журнали, визначення інцидентів, та аномальних подій. Зазвичай організації вибирають ELK Stack через те що цей продукт має модульну основу і містить декілька інструментів які можна вилучити або модифікувати у разі необхідності.

Інтегруючи компоненти Elasticsearch, Logstash і Kibana до інфраструктури організації вони будуть відповідати за наступні функції: Elasticsearch – це ядро всієї системи, яке поєднує в собі функції бази даних, пошукової та аналітичної системи; Logstash – це конвеєр обробки даних на стороні сервера, який може отримувати дані з декількох джерел одночасно, обробляти лог, а потім відправляє в базу даних Elasticsearch; Kibana дозволяє користувачам візуалізувати дані за допомогою діаграм і графіків в Elasticsearch, а також є можливість адмініструвати базу даних через зручний інтерфейс.

Великі чи маленькі організації можуть використовувати ELK Stack для управління загрозами, виявленням та розслідуванням кіберінцидентів, щоб швидко передавати інформацію про події, та швидко усувати наслідки. Команда, що відповідає за безпеку, повинна реагувати на кількість щоденних складних кібератак та на їхню організацію. Це послугувало причиною розгляду методів та засобів, які можуть автоматизувати процеси для скорочення часу як на стримування

інцидентів, так і на повне усунення нападу, що стосується кібербезпеки.

Отже, за допомогою програмних продуктів компанії Elastic можна створити чіткий механізм, який реалізовував би захист інформації для усунення слабких місць в інфраструктурі організації та швидке реагування спеціалістів з кібербезпеки на інциденти.

Література:

1. Elastic Stack[Електронний ресурс] – Режим доступу до ресурсу: https://www.elastic.co/elastic-stack

2. Deploying of infrastructure and technologies for a SOC as a Service (SOCasS)[Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@ibrahim.ayadhi/deploying-of-infrastructure-and-technologies-for-a-soc-as-a-service-socass-8e1bbb885149

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ МОЖЛИВОСТЕЙ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Гізун Ігор Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Чому процеси виявлення загроз та реагування настільки складні? Відповідь є одночасно простою і складною. Проблема полягає лише в тому, що кібератаки продовжують зростати в обсязі та витонченості. Простіше кажучи, вони ніколи не закінчуються, і вони продовжують вдосконалюватися для збільшення своєї ефективності та ускладнення виявлення. Понад три чверті (76%) спеціалістів вважають, що виявлення загрози та реагування на інцидент сьогодні складніші, ніж це було лише два роки тому. Це вражаючий результат, особливо зважаючи на величезну кількість уваги, ресурсів та інвестицій, витрачених протягом останніх кількох років на стратегії та продукти захисту для забезпечення кібербезпеки – і це потенційно може підтвердити, що ситуація може тільки погіршитися в майбутньому [1].

Загрози інформаційної (комп'ютерної) безпеки – це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами – це потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам [2].

Загрози ІБ можна розділити на два типи: природні і штучні. До природних відносяться природні явища, що не залежать від людини, наприклад урагани, повені, пожежі і т.д. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними та ненавмисними. Ненавмисні загрози виникають через необережність, неуважність та незнання. Прикладом таких загроз може бути установка програм, що не

входять в число необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і зсередини компанії. Результат реалізації цього виду загроз – втрати коштів та інтелектуальної власності компанії.

Все частіше зловмисники переходять від атак “в лоб” до більш складних і розподілених сценаріїв (APT - Advanced Persistent Threat). Загальні принципи, на яких будується APT, давно відомі. Наприклад, застосування соціальної інженерії, щоб спровокувати користувача перейти за посиланнями та відкрити прикріплений файл. Також зловмисники можуть використовувати вразливості для отримання доступу до системи. Проблема ж у тому, що в разі подібної атаки всі засоби захисту можуть мовчати, так як вирвані з контексту інциденти не будуть сприйматися як серйозна загроза. Але в той же самий час, аналіз сукупності інцидентів може явно вказати на атаку. Саме ці властивості приписують сучасним SIEM-системам – здатність виявляти атаки по частинкам, аномаліям, пост-аналізу подій і т.д. Система SIEM не спроможна самостійно запобігати інцидентам, як і не має вбудованих захисних функцій. Призначення даної системи полягає в аналізі даних, що надходять від різних інших систем, , таких як Intrusion Detection System (IDS), Data Leak Prevention (DLP), міжмережевих екранів, антивірусів, активного мережевого обладнання, системи контролю доступу і аутентифікації, сканерів вразливостей, і т. д. а також реєстрації і повідомлення про інцидент при виявленні відхилення від норм за заздалегідь заданими критеріями.

Універсальність системи SIEM обумовлюється гнучкістю її логіки. Однак для її ефективного функціонування необхідні корисні джерела і ретельно написані правила кореляції.

Саме вони, в сукупності з розміром накопиченої статистики в базі, в подальшому визначать кількість хибно-позитивних спрацювань системи, які, на жаль, неминучі на момент початку її експлуатації. Як джерело вхідної інформації для SIEM може бути використана практично будь-яка подія.

Збір даних від джерел в SIEM системі здійснюється встановленими на них агентами. У разі відсутності колектора відповідного джерела, події можуть бути відправлені в форматі стандарту Syslog. Основним завданням SIEM є своєчасне виявлення, оперативне реагування та запобігання загрозам. Для цього необхідно складання правил кореляції з урахуванням

актуальних для компанії ризиків, а також постійна актуалізація самих правил фахівцями.

В цілому загрози кібербезпеки можуть завдавати шкоди та збитків корпоративним інформаційним системам. Основні джерела загроз – хакери, намагаються отримати доступ до систем організацій з метою крадіжки даних, коштів або виведення з ладу обладнання.

SIEM-системи дозволяють домогтися практично повної автоматизації процесу виявлення загроз, але при не правильному налаштуванні призводять до нераціональної витрати коштів.

Література:

1. The Growing Challenges of Threat Detection and Response [Електронний ресурс] – Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/growing-challenges-threat-detection-and-response.

2. Кибербезопасность 2019-2020. Тренды и прогнозы [Електронний ресурс] – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020.

ШЛЯХИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Гізун Ігор Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

На сьогоднішній день процеси виявлення загроз та реагування залишаються складними. Проблема полягає лише в тому, що кібератаки продовжують зростати в обсязі та витонченості. Тобто, вони продовжують вдосконалюватися для збільшення своєї ефективності та ускладнення виявлення. Це передбачає потребу у пошуку шляхів виявлення вразливостей та забезпечення захисту корпоративних інформаційних систем.

Понад три чверті (76%) спеціалістів вважають, що виявлення загрози та реагування на інцидент сьогодні складніші, ніж це було лише два роки тому. Це вражаючий результат, особливо зважаючи на величезну кількість уваги, ресурсів та інвестицій, витрачених протягом останніх кількох років на стратегії та продукти захисту для забезпечення кібербезпеки – і це потенційно може підтвердити, що ситуація може тільки погіршитися в майбутньому [1].

Загрози інформаційної (комп'ютерної) безпеки – це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами – це потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам [2].

Загрози ІБ можна розділити на два типи: природні і штучні. До природних відносяться природні явища, що не залежать від людини, наприклад урагани, повені, пожежі і т.д. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними та ненавмисними. Ненавмисні загрози виникають через необережність, неуважність та незнання. Прикладом таких загроз може бути установка програм, що не входять в число необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і зсередини компанії. Результат реалізації цього виду загроз – втрати коштів та інтелектуальної власності компанії.

Все частіше зловмисники переходять від атак «в лоб» до більш складних і розподілених сценаріїв (APT – Advanced Persistent Threat). Загальні принципи, на яких будується APT, давно відомі. Наприклад, застосування соціальної інженерії, щоб спровокувати користувача перейти за посиланнями та відкрити прикріплений файл. Також зловмисники можуть використовувати вразливості для отримання доступу до системи. Проблема ж у тому, що в разі подібної атаки всі засоби захисту можуть мовчати, так як вирвані з контексту інциденти не будуть сприйматися як серйозна загроза. Але в той же самий час, аналіз сукупності інцидентів може явно вказати на атаку. Саме ці властивості приписують сучасним SIEM-системам – здатність виявляти атаки по частинкам, аномаліям, пост-аналізу подій і т.д. Система SIEM неспроможна самостійно запобігати інцидентам, як і не має вбудованих захисних функцій. Призначення даної системи полягає в аналізі даних, що надходять від різних інших систем,, таких як IntrusionDetectionSystem (IDS), DataLeakPrevention (DLP), міжмережевих екранів, антивірусів, активного мережевого обладнання, системи контролю доступу і аутентифікації, сканерів вразливостей, і тощо, а також реєстрації і повідомлення про інцидент при виявленні відхилення від норм за заздалегідь заданими критеріями.

Універсальність системи SIEM обумовлюється гнучкістю її логіки. Однак для її ефективного функціонування необхідні корисні джерела і ретельно написані правила кореляції.

Саме вони, в сукупності з розміром накопиченої статистики в базі, в подальшому визначать кількість хибно-позитивних спрацювань системи, які, на жаль, неминучі на

момент початку її експлуатації. Як джерело вхідної інформації для SIEM може бути використана практично будь-яка подія.

Збір даних від джерел в SIEM системі здійснюється встановленими на них агентами. У разі відсутності колектора відповідного джерела, події можуть бути відправлені в форматі стандарту Syslog.и Основним завданням SIEM є своєчасне виявлення, оперативне реагування та запобігання загрозам. Для цього необхідно складання правил кореляції з урахуванням актуальних для компанії ризиків, а також постійна актуалізація самих правил фахівцями.

В цілому загрози кібербезпеки можуть завдавати шкоди та збитків корпоративним інформаційним системам. Основні джерела загроз – хакери, намагаються отримати доступ до систем організацій з метою крадіжки даних, коштів або виведення з ладу обладнання.

SIEM-системи дозволяють домогтися практично повної автоматизації процесу виявлення загроз, але при не правильному налаштуванні призводять до нераціональної витрати коштів.

Література:

1. The Growing Challenges of Threat Detectionand Response[Електронний ресурс] – Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/growing-challenges-threat-detection-and-response.

2. Кибербезопасность 2019-2020. Тренды и прогнозы [Електронний ресурс]– Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020.

ВИКОРИСТАННЯ МОДЕЛІ БАГАТОРІВНЕВОЇ СИСТЕМИ ДОСТУПУ

Гінько Артем Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Мета дослідження полягає у вирішенні науково-прикладної задачі побудови інформаційних засобів захисту даних в інформаційних системах [1] на основі використання багаторівневої системи надання повноважень користувачам [2].

Дворівнева модель надання повноважень на використання даних різних рівнів конфіденційності функціонує наступним чином. На першому рівні надання повноважень відповідна система аналізує повноваження користувача, який звертається до системи для отримання даних. Перевіряються ідентифікаційні дані користувача та дані, що визначають його право на доступ до даних певних рівнів конфіденційності.

Користувач, який звертається до системи, крім власних даних, повинен надати системі відомості про задачу, для розв’язання якої потрібні відповідні дані. У випадку, коли дані, за якими звернувся користувач, відносяться до вищих рівнів конфіденційності і не повинні надаватися користувачу, то система надання повноважень переходить на другий рівень. На цьому рівні функції користувача виконує прикладна задача, що була представлена користувачем – фізичною особою, і в цьому випадку така задача називається користувачем – задачею. На цьому рівні система надання повноважень проводить аналіз параметрів інформаційних запитів задачі і на його основі приймає рішення про можливість надання даних задачі або ж приймає рішення щодо забезпечення умов, які гарантують можливість вирішення зазначеної задачі. Важливим аспектом функціонування системи надання повноважень на другому рівні є те, що користувач – фізична особа не має можливості впливати на прийняття системою рішення щодо надання повноважень на отримання даних задачею або сприяти забезпеченню можливості розв'язання цієї задачі. Це означає, що під час роботи з даними високого рівня конфіденційності у користувача відсутня можливість вплинути на розв'язання задачі, виходячи з певних суб'єктивних факторів чи інших причин, які можуть мати відношення до нього.

На другому рівні надання доступу відповідна система може виконувати цілий ряд функцій із забезпечення процесу розв'язання прикладної задачі. Для реалізації таких функцій система надання повноважень аналізує дані про предметну область інтерпретації, яку вона обслуговує. Прикладом однієї з можливостей із забезпечення розв’язання прикладної задачі може слугувати наступна можливість системи. Для обраного рівня конфіденційності даних система містить алгоритми, якими можуть перетворюватися відповідні дані. Система надання повноважень обирає алгоритм перетворення даних, який найбільшою мірою відповідає фрагменту алгоритму, що реалізується в задачі і призначений для перетворень цих даних, за якими звертається задача, та за результатами чого здійснює відповідні перетворення даних. Завдяки цьому система не передає дані задачі, а передає їй результат перетворення відповідних даних, який має рівень конфіденційності нижчий, ніж рівень конфіденційності даних, які перетворювалися. Цей підхід ґрунтується на тому, що дані відповідного рівня конфіденційності можна перетворювати тільки обмеженою кількістю алгоритмів. Це обмеження встановлюється на основі

аналізу інтерпретації відповідних даних у предметній області інтерпретації, яку обслуговує відповідна інформаційна система.

Для реалізації процесу побудови багаторівневої моделі надання повноважень водиться ряд положень, які визначають умови використання відповідної системи. Прикладом такого положення є вимога, яка стосується необхідності інтерпретації даних, які використовуються прикладними задачами, які узгоджуються з інтерпретаціями компонентів, що входять до складу предметної області інтерпретації, та обслуговуються інформаційною системою. Доводяться твердження про обмеженість множини критичних ситуацій та аномалій, які можуть виникати в предметній області інтерпретації інформаційної системи. Доводяться також твердження про те, що система засобів, які використовуються системою надання повноважень на використання відповідних даних, є повною відносно задач. У роботі приймається, що необхідність тих чи інших рівнів конфіденційності даних визначається можливим рівнем втрат. До цих втрат може призвести використання результатів розв'язання, які отримані несанкціонованими прикладними задачами. Використання цих результатів може відбуватися лише в предметній області інтерпретації інформаційної системи.

Важливим компонентом системи надання повноважень є система прийняття рішень, використання якої дозволяє співпрацювати з прикладною задачею, яка потребує даних, що мають найвищі рівні конфіденційності. Оскільки необхідний рівень конфіденційності даних визначається рівнем втрат, до яких може призвести використання результатів, отриманих несанкціонованими задачами у відповідній предметній області інтерпретації, що використовує відповідні дані, то можливість пониження рівня конфіденційності даних, при використанні результатів розв’язання санкціонованих задач, може призвести до підвищення рівня безпеки інформаційної системи, що безпосередньо пов'язана з безпекою процесів, які відбуваються в предметній області інтерпретації цієї інформаційної системи.

Література:

1. *Давиденко А.М. Використання формальних засобів опису процесів надання повноважень / А.М. Давиденко, О.А. Суліма // Захист інформації – Київ, 2016. - Том 18. - №2. - С.143-149*

2. *Суліма О.А. Модель багаторівневої системи доступу / О.А. Суліма // Безпека інформації – Київ, 2017. –Том 23. – с. 123-130.*

СТАНДАРТИЗАЦІЯ У СФЕРІ ТЕЛЕКОМУНІКАЦІЙ

Грабовий Вадим Андрійович

Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

На початку розвитку телекомунікацій з'явилась проблема, яка полягала в тому, що мережеве обладнання, яке вироблялось різними фірмами, не було сумісне один з одним. Для вирішення цієї проблеми було створено ряд організацій та форумів, які займаються розробленням стандартів та специфікацій. Роботи зі стандартизації були розпочаті ще в 70-х рр. Існують як міжнародні, так і національні організації із стандартизації у сфері телекомунікацій.

Основною метою стандартизації у сфері телекомунікацій є визначення вимог до телекомунікаційних мереж, їх технічних засобів та якості послуг, які вони надають. Для цього була створена єдина система державних і галузевих стандартів, які мають тісно співвідноситись з міжнародними нормативними документами [1].

На сьогоднішній день існує велика кількість міжнародних та національних організацій, які займаються розробкою стандартів та рекомендацій для комп'ютерних мереж та систем комунікації. В залежності від статусу організацій виділяють такі види стандартів [2]:

- *міжнародні стандарти* (ITU, ISO, IEC та інші);
- *національній стандарти* (ANSI, IEEE, ISA тощо);
- *стандарти спеціальних комітетів, об'єднань та форумів*, які створюються декількома фірмами, наприклад, стандарти технології ATM, розроблені спеціально створеним об'єднанням ATM Форум, стандарти союзу Fast Ethernet та інші;
- *стандарти окремих компаній та фірм* (наприклад, стек протоколу DECnet, фірми Digital Equipment тощо);

На основі міжнародних стандартів розроблюються національні, які можуть бути більш конкретнішими. Ці стандарти є основою розробки мережних технічних і програмних засобів. Розвиваючись, деякі стандарти можуть переходити з однієї категорії в іншу [3].

Нижче подані назви й основні відомості щодо організацій, які є одними з найбільш відомих своєю активністю та успішністю.

Міжнародний союз електрозв'язку **(МСЕ)** або ***International Telecommunications Union*** **(ITU)**. Міжнародний союз електрозв'язку визначає політику стандартизації й регламентації в цій сфері телекомунікацій. Рекомендації ITU спрямовані на гармонізацію технічних рішень, стандартизацію протоколів для організації міжнародних зв'язків. ITU був створений у 1865 р. й до 1934 р. називався Міжнародним телеграфним союзом. З 1947 р. ITU — спеціалізована установа Організації Об'єднаних Націй (ООН). Нині в його роботі беруть

участь всі країни — члени ООН. До ITU входить близько двохсот держав, кожна з яких представлена в Союзі повноважними органами. Вищий орган ITU — Повноважна конференція, скликається раз на чотири роки й визначає стратегію роботи ITU. У ній беруть участь делегації всіх членів ITU. У періоди між повноважними конференціями проводяться щорічні засідання Ради ITU. Рада ITU поєднує 25 % від загальної кількості держав — членів ITU, які обираються Повноважною конференцією відповідно до вимоги об'єктивного розподілу місць у Раді між п'ятьма регіонами світу (Америкою, Західною і Східною Європою, Африкою, Азією і Австралією) [4].

Міжнародна організація по стандартизації **ISO *(International Organization for Standardization)***, яка на сьогодні об`єднує 163 держави, створена в 1946 році. Сфера діяльності ISO стосується стандартизації у всіх областях, крім електротехніки та електроніки, які відносяться до компетенції міжнародної електротехнічної комісії (IEC – International Electrotechnical Commission). Крім стандартизації ця організація займається проблемами сертифікації. ISO є домінуючою організацією по стандартизації в області інформаційних технологій і розробила та затвердила безліч стандартів, в тому числі для мережевих технологій. Документи, які прийнято ISO, мають статус міжнародного стандарту і позначаються номером, наприклад, ISO 10026. Зокрема, цій організації належить розробка еталонної моделі взаємодії відкритих систем OSI (Open System Interconnection) – абстрактної мережевої моделі для комунікацій і розробки мережевих протоколів, яка представляє мережу як сукупність рівнів, кожний з яких визначає і обслуговує свою частину взаємодії кінцевих станцій та передачі даних через мережу [2].

Інститут інженерів з електротехніки і радіоелектроніки **(IEEE)** — національна організація США, що визначає мережні стандарти. В 1981 р. робоча група 802 цього інституту сформулювала основні вимоги, яким мають задовольняти локальні мережі зв'язку. Група 802 визначила множину стандартів, з них найвідомішими є стандарти 802.1, 802.2, 802.3 і 802.5, які описують загальні поняття, що використовуються в галузі локальних мереж, а також стандарти на два нижні рівні мереж Ethernet і Token Ring [4].

Американський національний інститут стандартів **ANSI (*American National Standards Institute*)** – некомерційна неурядова організація, яка розробляє та публікує стандарти для промисловості країни. Інформаційними технологіями займаються наступні комітети [2]:

- ***JTC1 TAG*** – технічна консультативна група ***(Technical Advisory Group)***, яка представляє позицію США по стандартам в ISO;

- ***ASC X.3***, який розробляє 90 % стандартів США в області інформаційних технологій; підкомітет X.3 відповідає за стандартизацію технології ***FDDI (Fiber Distributed Digital Interface)***;

- ***ASC T.1*** – добровільний орган стандартизації для телекомунікаційної галузі США, який розробляє національні телекомунікаційні стандарти;

- ***ASC X.12*** – група відповідає за стандарти, які відносяться до електронного обміну даними (EDI – Electronic Data Interchange) на території США.

Вимоги державних і галузевих стандартів, інших нормативних документів щодо технічних засобів телекомунікацій є обов'язковими для всіх виробників і постачальників технічних засобів, науково-дослідних, проектних та будівельних організацій, а також для операторів, провайдерів телекомунікацій. Вимоги до якості послуг є обов'язковими для операторів, провайдерів телекомунікацій, що надають телекомунікаційні послуги на території України. Галузеві стандарти розробляються та затверджуються відповідно до законодавства України про стандартизацію з урахуванням стандартів та рекомендацій міжнародних організацій [1].

Отже, без повного узгодження та дотримання загальноприйнятих стандартів для обладнання і протоколів між всіма учасниками телекомунікаційного ринку, не було б прогресу у справі побудови інфокомунікаційних мереж.

Література:

1. Стандартизація у сфері телекомунікацій [Електронний ресурс] – Режим доступу до ресурсу: https://protocol.ua/ua/pro_telekomunikatsii_stattya_25/.

2. Стандартизація мереж [Електронний ресурс] – Режим доступу до ресурсу: http://www.scs.kpi.ua/sites/default/files/standartizaciya_merezh.doc.

3. Стандартизація в галузі телекомунікацій. Організації — розробники стандартів: міжнародні, європейські, національні [Електронний ресурс] – Режим доступу до ресурсу: http://osvita-plaza.in.ua/publ/45-1-0-434.

4. Стисла характеристика організацій зі стандартизації [Електронний ресурс] – Режим доступу до ресурсу: https://www.znanius.com/3588.html.

SYN-FLOOD АТАКА. РЕАЛІЗАЦІЯ ТА ЗАХИСТ

Гребенюк Владислав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Деякі провайдери (і чим далі, тим більше таких з'являється) фільтрують трафік своїх клієнтів на предмет підробки адреси відправника. Є велика ймовірність, що возможнось спуфинга обмежується підмережею класу С. Крім того, хост, адреса якого вказується в запиті на підключення, не повинен реагувати на відповіді сервера - найпростіше вибрати адресу, на якому немає машини. При практичної реалізації, особливо створюючи універсальний інструмент для координованої атаки, потрібно враховувати ці дві особливості, і проводити атаку тільки зі своєю підмережі і з тих адрес, які не відповідають. Ще одна проблема - для проведення атаки необхідно мати адміністраторські привілеї.

Проблеми, які не залежать від атакуючого.

Деякі провайдери (і чим далі, тим більше таких з'являється) фільтрують трафік своїх клієнтів на предмет підробки адреси відправника. Є велика ймовірність, що возможнось спуфинга обмежується підмережею класу С. Крім того, хост, адреса якого вказується в запиті на підключення, не повинен реагувати на відповіді сервера - найпростіше вибрати адресу, на якому немає машини. При практичної реалізації, особливо створюючи універсальний інструмент для координованої атаки, потрібно враховувати ці дві особливості, і проводити атаку тільки зі своєю підмережі і з тих адрес, які не відповідають. Ще одна проблема - для проведення атаки необхідно мати адміністраторські привілеї.

Програмна реалізація.

Для реалізації підходить як unix, так і windows-платформи. Програма повинна запускатися з правами root і адміністратора відповідно. Під unix багато готових реалізацій, наприклад, synk4.c (шукати пошуковими системами). Спеціалізовані для координування DDoS-атак реалізації знайти складніше, але при мінімальних навичках програмування можна доопрацювати існуючі або створити свої.

Крім стандартних сирих сокетів, D0minat0r з Nerf знайшов дуже гарний спосіб реалізації SYN flood під linux, на інших юніксоподобних не пройшло перевірку, на win не працює. Linux дозволяє root'у биндить сокет до будь-якою адресою, в т.ч. що не належить локальному хосту. Після цього можна викликати connect () для цього сокета, і локальний хост пошле SYN-пакет від адреси, до якого прібінжен сокет. Якщо сокет був в неблокірующіх режимі, то відразу після connect () можна викликати close (), і повторювати операцію.

Реалізації під windows зустрічаються рідше, через поширеної міфу про неможливість генерації сирих пакетів в цій OS. Насправді, win98 підтримує сирі сокети рівня до заголовка IP, а win2k і XP - і заголовок теж (опція IP_HDRINCL), тобто реалізація атаки під win2k і XP відрізняється від юніксовской лише кількома рядками. Готова реалізація від мене, перевірена

на win2k, лежала у свій час на www.nerf.ru, але після зміни хостингу, як я пішов з цієї групи і Форматцевт загубилася. Якщо у кого-то збереглася - зв'яжіться, плиз, викладу.

Механізми захисту OS від SYN-flood.

а) Стандартний таумаут. Напіввідкриті з'єднання після деякого часу викидаються з буфера. При виснаженні буфера запити клієнтів на підключення будуть проходити з ймовірністю C1 / C2, де C1 - кількість SYN-пакетів від клієнта, C2 - кількість SYN-пакетів від всіх інших (включаючи атакуючого). Навіть при навантаженні на канал атакуючого в 6 пакетів в секунду C1 / C2 - приблизно 1/100, тобто служба виведена з ладу на 99%.

б) Безлімітний буфер напіввідкритих з'єднань. При навантаженні на канал атакуючого 100 Mb / сек і таймаут близько хвилини чергу напіввідкритих з'єднань буде займати приблизно 1 Gb пам'яті, що для великих серверів не смертельно. Побічний ефект: атакується сервер відповідає трафіком, в 3 рази більшим, ніж трафік атакуючого (кажуть, що відбувається DDoS з множенням в 4 рази), що може призвести до виснаження пропускної здатності каналу. Однак, при неможливості виснажити ширину каналу, захист від атаки буде абсолютною, жодне клієнтське з'єднання не буде відкинуто.

в) Очищення найбільш старих напіввідкритих з'єднань. При переповненні буфера з нього видаляються найстаріші напіввідкрите з'єднання. Побічний ефект: якщо при атаці буфер заповнюється за час t, то клієнт не зможе підключитися під час атаки, якщо час підтвердження з'єднання більше t - його запит теж буде викинутий. Наприклад, для навантаження каналу атакуючого 4 Мбіт / сек і довжини буфера 512 (рекомендоване значення для Win2K) час t - близько 50 msec, що гарантовано відкине всі спроби підключення до сервера з діалапу і багато - з виділених ліній. Збільшуючи розмір буфера, захист можна звести до попереднього варіанту.

г) SYN COOKIE. Після виснаження буфера інформація, яка не поміщається в буфер, відсилається клієнту, який нібито запросив її. Якщо клієнт - справжній, то він повертає інформацію назад, якщо підроблений - вона втрачається, причому механізм реалізований в рамках RFC по TCP, тобто його підтримують і клієнти, які не знайомі з цією технологією. Операційна система с SYN COOKIE, незалежно від розміру буфера напіввідкритих з'єднань, абсолютно невразлива для SYN-flood атак. Побічний ефект: заборона "великих вікон".

Резюме: SYN-flood атака морально застаріла, і сьогодні може використовуватися в кращому випадку в якості звичайної flood-атаки на перевищення пропускної здатності каналу.

Література:
1. SecurityLab. syn-flood атака – практика / Режим доступу: [https://www.securitylab.ru/analytics/216198.php]

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Гридяєва Вероніка Русланівна
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

В світлі розвитку нових IT-технологій, поняття інформаційної безпеки значно розширилося. Деякі експерти вказують на те, що більш доцільно повністю замінити поняття інформаційної безпеки поняттям кібербезпеки. Це пов'язано з тим, що сьогодні від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації. Тобто втрата інформації тягне за собою ряд інших комплексних ускладнень. Кібербезпека — це захист від вірусів, хакерських атак, підробки даних. Адже віруси, наприклад, можуть не тільки видалити чи вкрасти дані, але і вплинути на роботу і продуктивність співробітників чи навіть зупинити виробництво. Більше того, зважаючи на широку інтеграцію цифрових технологій в життя і тіло людини, питання інформаційної безпеки стає подекуди питання життєвої безпеки.

Досвід протидії загрозам безпеки та побудови систем управління інформаційними ризиками, використання системного підходу до аналізу захищених інформаційних систем дозволив сформулювати основні науково-практичні принципи забезпечення інформаційної безпеки.

1. Забезпечення інформаційної безпеки виконується відповідно до політики управління інформаційними ризиками, розробка і реалізація якої здійснюється під безпосереднім керівництвом перших осіб підприємства із залученням менеджменту відповідних служб і відділів.

2. Архітектура системи управління інформаційними ризиками (СУІР) забезпечує оптимальний (раціональний) баланс витрат на управління інформаційними ризиками і загального збитку від інформаційних ризиків.

3. Система управління інформаційними ризиками є централізованою і реалізує єдину політику управління.

4. Безпека інформації досягається за рахунок комплексного використання нормативних, економічних та організаційних заходів, технічних, програмних і криптографічних засобів.

5. Система управління повинна бути багаторівневою і рівно захищеною у всіх ланках.

6. Повинна бути забезпечена безперервність функціонування на всіх життєвих циклах системи.

7. Повинно бути забезпечено розмежування та обмеження доступу персоналу до інформації.

8. Система повинна бути здатна до розвитку та адаптації до зміни умов функціонування.

9. Наявність системи безперервного моніторингу за виконанням всім персоналом встановлених правил роботи в інформаційній системі.

10. Моніторинг і аудит ефективності системи і своєчасна її модернізація.

Політика підприємства повинна відповідати вимогам законодавства. Для державних організацій безпека інформації забезпечується відповідно до вимог національних стандартів та інших керівних документів державних організацій - регуляторів сфери інформаційної безпеки держави.

Система управління інформаційними ризиками підприємства повинна бути ієрархічно централізованою для забезпечення єдиної політики управління у всіх підрозділах (у тому числі і територіально рознесених).

Не існує одного методу, які міг б забезпечити 100% захист від загроз безпеки інформації. Для підвищення ефективності системи необхідно комплексно використовувати комбінації методів і засобів захисту різної природи і принципів дії. При цьому слід мати на увазі, що основою для створення системи захисту є нормативна правова база, а всі засоби захисту будуть ефективні, якщо в системі налагоджено узгоджене виконання організаційних заходів, алгоритмів і дій всіма співробітниками. Висока захищеність інформаційної системи досяжна тільки при використанні багаторівневої системи захисту від загроз. В таких системах зловмисникові потрібно подолати кілька бар'єрів на шляху до інформації.

Важливо при побудові СУІР виключити наявність слабких ланок у системі захисту. Зловмисник буде старатись знайти найменш захищений елемент системи захисту для виконання свого задуму. Тому надійність всієї системи захисту визначається надійністю найслабшого елемента. Це справедливо і для випадкових загроз. Прорив водозахисної дамби, пробій електроізоляційних матеріалів, займання горючих матеріалів мають місце в найменш захищених місцях. У період експлуатації інформаційної системи, незалежно від режиму роботи і тимчасових рамок, вона повинна бути відповідним

чином захищена від можливих загроз безпеці інформації. Безперервність захисту поширюється також на всі етапи роботи з інформацією - введення, зберігання, обробку, видачу, передачу.

Одним з основних принципів забезпечення інформаційної безпеки є обмеження і розмежування доступу персоналу до важливої інформації. Кожному працівникові мають делегуватися мінімально можливі права з доступу до ресурсів системи в суворій відповідності з його функціональними обов'язками. Важливо, щоб всі співробітники знали, що їхні дії в інформаційній системі можуть бути в будь-який момент часу проконтрольовані, а частина найбільш відповідальних дій і подій задокументована. Керівництво підприємства зобов'язане організувати моніторинг і періодичний аудит ефективності функціонування СУІР і, при необхідності, своєчасно забезпечити модернізацію системи

***Література**:*

1. https://stud.com.ua/53393/informatika/printsipi_zabezpechennya_informatsiynoyi_bezpeki

2.https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0

МЕХАНІЗМ АВТЕНТИФІКАЦІЇ WEB-САЙТІВ ТА ЙОГО ВРАЗЛИВОСТІ

Грищенко Ярослав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

В наш час в Європейському Союзі ведуться інтенсивні розробки, які пов'язані з надання транскордонних та електронно-довірчих послуг. Однією з базових послуг, що розробляється, є послуга електронної автентифікації web-сайту. На сьогоднішній день, дуже велика кількість компаній використовує сайти в мережі Інтернет для своїх цілей. Власники сайтів можуть розміщувати там конфіденційну інформацію, доступ до якої обмежений. Для цього захисту використовують різні механізми автентифакації web-сайтів, що дозволяють здійснити виконання основних вимог захисту інформації.

Метою даної доповіді є аналіз протоколу SSL\TLS як механізм захисту електронних довірчих послуг, а також його існуючі вразливості та методи захисту, які зможуть підвищити стійкість до цих атак.

Протокол автентифікації web-сайтів SecureSocketsLayer / TransportLayerSecurity

Протоколи SSL / TLS - це криптографічні протоколи, завданням якого є виконання криптографічного перетворення

даних інформації. Автентифікація ґрунтується на пред'явлення X. 509-сертифіката, або ланцюжка сертифікатів. Конфіденційність забезпечується шифруванням переданих даних, а цілісність - передачею з кожним блоком переданих даних обчисленого значення хеш-функції.

Протокол SSL (secure sockets layer - шар безпечних з'єднань) - це протокол взаємодії інформаційних серверів і універсальних клієнтів по захищеному каналу зв'язку. Для двох взаємодіючих додатків протокол забезпечує аутентифікацію та ідентифікацію сервера і клієнта, шифрування даних, контроль цілісності повідомлення. Він підтримує встановлення автентичності як на рівні сервера, так і на рівні клієнта.

Протокол TLS (transport layer security) забезпечує безпеку передачі даних між вузлами в мережі Інтернет. Так само, як і протокол SSL, він відноситься до протоколів транспортного рівня. Його можна розглядати як розвиток протоколу SSL. Робота протоколу TLS заснована па специфікації протоколу SSL версії 3.

TLS і SSL - це протоколи, що забезпечують криптографічний захист даних при їх передачі між вузлами в мережі Інтернет. Вони використовують асиметричні методи криптографічного захисту для аутентифікації і симетричні методи криптографічного захисту для забезпечення конфіденційності, а також гарантують цілісність повідомлень.

В електронній торгівлі протокол використовується для передачі магазину інформації про платіжну картку клієнта або для захищеного обміну даними. Протокол забезпечує захист тільки від зовнішніх впливів зловмисників, припускаючи повна довіра один одному продавця і покупця. Це характерно для здійснення угод на невелику суму.

Протокол TLS відрізняється від SSL тим, що в ньому:

✓використовується інший алгоритм обчислення коду автентичності повідомлень;

✓розширено набір кодів сповіщень;

✓інші методи криптографічних обчислень (ключів цифрових підписів).

Вразливості SSL\TLS та можливі заходи для підвищення стійкості

В даній частині будуть розглянуті найбільш небезпечні загрози для протоколу SSL\TLS та їх алгоритми зламу web-сайтів. На основі цих атак буде відтворення можливих перешкод для реалізації цих атак.

Для використання протоколу **SSL** необхідно придбати в одному з центрів сертифікації цифровий сертифікат і встановити

його на сервер. При використанні цього протоколу для забезпечення безпеки передачі даних:

✓ дані шифруються. Так, при відправці користувачем номера банківської пластикової карти із застосуванням протоколу SSL дані шифруються, і хакер не зможе прочитати їх зміст;

✓ між сервером-джерелом і сервером призначення встановлюється захищене з'єднання;

✓ активується аутентифікація сервера.

Висновки. На даний момент існує багато протоколів автентифікації web-сайтів, які допоможуть нам забезпечити для забезпечення основних функцій. Але з часом, ці протоколи становляться ненадійними, тому створюються нові протоколи. І таким чином, йде розвиток напрямку кібербезпеки. Протоколи автентифікації SSL/TLS задовольняють вимоги стійкості, хоча є деякі слабкості, які використовувалися на основі сімейств протоколів SSL та TLS, але на даний момент проводяться модифікації даного протоколу та виправляються ці слабкості.

Література:

1. В.Г. Грибунин, И.Н. Оков, И.В. Туринцев, Цифровая стеганография, М: Солон-Пресс, 2002 г.

2. Закон України «Про електронні довірчі послуги» від 14 січня 2015 р.

3. Доктрина інформаційної безпеки №47/2017 від 25 лютого 2017 р.

4. Баранов О.А. Інформаційне право України: Стан, проблеми, перспективи. -К.: Видавничий дім «СофтПрес», 2005. - 316с.

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ КОРПОРАТИВНИХ МЕРЕЖ

Данильченко Юлія Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Метою роботи було розробити рекомендації щодо захисту конфіденційних даних корпоративних мереж. Для цього було опрацьоване Законодавство України та Європи, виконано їх порівняння, вивчення літератури за даною темою, аналіз експлуатаційної та технічної документації. Було проведено аналіз проблеми забезпечення захисту конфіденційної інформації в корпоративних мережах. На основі дослідження було розроблено рекомендації щодо захисту конфіденційних даних корпоративних мереж. Найважливішою метою кібербезпеки є захист інформації від витоку, спотворення, знищення та оприлюднення, тому тема роботи є актуальною.

Ключові слова: корпоративна мережа, захист конфіденційної інформації, запобігання витоку інформації, DLP-системи.

За визначенням поняття конфіденційної інформації можна звернутись до двох законів, а саме до Закону «Про доступ до публічної інформації» та Закону «Про інформацію».

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень [1]. Тільки особи приватного права можуть вирішувати, яка інформація про них є конфіденційною, а яка відкритою. Але іноді законами передбачається неприхованість певної інформації. На підприємстві найбільш цінується інформація про виробництво і продукцію, про ринок на який спрямована робота фірми, матеріально технічне забезпечення, систему безпеки фірми і т.д.

При розробці рекомендацій слід звернути увагу і на міжнародне законодавство, а саме на Генеральний регламент про захист персональних даних (англ. General Data Protection Regulation, GDPR). Цей документ ЄС діє по всьому світу, передбачає значне посилення вимог щодо забезпечення захисту персональних даних та покладання за це відповідальності на організацію, якщо вона: запускає таргетовану рекламу на території ЄС, реалізує товари і послуги громадянам ЄС, приймає оплату в євро, відслідковує переваги потенційних покупців з ЄС, зареєстрована в одній із юрисдикцій ЄС [2].

Для створення рекомендацій також важливо знати які існують канали витоку інформації на підприємстві. Вони поділяються на: прямі і непрямі, фізичні та інформаційні, технічні.

Важливим способом збереження інформації на підприємстві є створення резервних копій та відновлення по ним втрачених даних. Резервне копіювання поділяється на декілька видів за кількістю витрат на це коштів і часу: повне резервне копіювання, інкрементне та диференціальне.

Для захисту конфіденційних даних на підприємстві використовуються DLP-системи (Data Leak Prevention або Data Loss Prevention) - програмні продукти, що захищають організації від витоків конфіденційної інформації. Вони виконують наступні функції: контроль передачі інформації через Інтернет, контроль збереження інформації на зовнішні носії, контроль виведення даних на друк, блокування спроб пересилання / збереження конфіденційних даних, інформування адміністраторів інформаційної безпеки про інциденти, створення тіньових копій, додавання файлів в карантинну папку, контроль життєвого циклу і руху конфіденційних відомостей.

IBM Security Guardium є програмним забезпеченням , яке підходить для реалізації захисту конфіденційної інформації будь-якого підприємства. Ця комплексна платформа дозволяє аналізувати події, які відбуваються в середовищі даних, щоб допомогти мінімізувати ризики, захистити конфіденційні дані

від внутрішніх і зовнішніх загроз і безперешкодно адаптуватися до змін, які впливають на безпеку і цілісність даних.

Функціональність і можливості системи можна розділити на кілька основних категорій:

1. Захист баз даних:

– Моніторинг і аудит всіх дій з даними;

– Застосування політик безпеки в режимі реального часу;

– Прискорення відповідності процесів і аудиту;

– Легка адаптація до змін в середовищі даних;

– Підтримка гетерогенних середовищ.

2. Захист даних в файлах і файлових системах:

– Моніторинг і аудит усіх дій з файлами;

– Прискорення відповідності процесів і аудиту;

– Захист файлів в гетерогенних середовищах;

– Застосування політик безпеки для доступу до файлів і контролю змін.

3. Виявлення вразливостей і аналіз ризиків.

4. Шифрування даних:

– Управління політиками доступу користувачів.

5. Інтеграція з іншими системами безпеки [3].

Основні рекомендації яким повинна слідувати компанія аби забезпечити захист інформації від витоку по корпоративним мережам виходячи з виконаного дослідження:

1. Компанія повинна розібратись у законодавчій базі України та Європи за приводу захисту конфіденційних даних.

2. Слід дослідити свою корпоративну мережу на рахунок можливих шляхів витоку конфіденційних даних.

3. Треба забезпечити захист мережевого обладнання. Для цього можна встановити захист у формі як фізичних механізмів, так і протоколів..

4. Також слід звернути увагу на резервне копіювання. Підібрати вид резервного копіювання звертаючи увагу на кількість витрат на це коштів і часу.

5. Підбрати програмне забезпечення яке буде здійснювати захист конфіденційної інформації підприємства. Для цієї задачі підійде IBM Security Guardium.

В даній роботі було проведено дослідження проблеми забезпечення безпеки корпоративних мереж від витоку конфіденційної інформації. Визначено, що дане питання є основним у безпеці компаній у яких присутні конфіденційні дані і потребує відповідального до цього ставлення. Були надані основні рекомендації яким повинна слідувати компанія для захисту конфіденційної інформації.

Література:

1. Про інформацію [Текст] : Закон України №2657- XII від 2 жовтня 1992 р. – Чин. 2019.12.21. / Верховна Рада України // Відомості Верховної Ради України. – 1992. — №48. — Ст. 650.

2. General Data Protection Regulation : Regulation (EU) 2016/679 Of The European Parliament and Of The Council of 27 April 2016. — Official Journal of the European Union. — 2018.

3. Secure the data that powers your business: Security. Solution Brief. — IBM Corporation, 2017. — 6 p.

ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ НА БАЗІ РІШЕНЬ ESET

Добреля Віталій Олексійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

В сучасному світі нові технології надзвичайно тісно пов'язані з побутовим життям людей. Сьогодні вже нікого не здивуєш покупками через Інтернет, миттєвим пошуком необхідної інформації, чи бронюванням авіаквитків онлайн. Така колаборація здійснюється і в різних сферах бізнесу. Разом зі зміною економічних відносин ми спостерігаємо зміну використання інформаційних технологій у напрямку зростання.

Дане питання постає особливо гостро на тлі пандемії, коли компанії все частіше задумуються про переведення бізнесу в онлайн. Зростання впливу інформаційних систем на бізнес зумовлює необхідність підвищення рівня безпеки інформаційних ресурсів. З огляду на це набувають необхідності дослідження теоретичних завдань та методичних рекомендацій з впровадження інформаційних технологій. Не менш важливими є дослідження з використання засобів та заходів для забезпечення безпеки інформаційних ресурсів підприємства.

Важливо розрізняти підходи до забезпечення кібербезпеки інформаційних ресурсів корпорацій та малого і середнього бізнесу. При розробці рекомендацій для малого та середнього бізнесу потрібно враховувати доцільність використання тих чи інших засобів з погляду на фінансову спроможність компанії та вартість інформаційних ресурсів.

Інформаційні системи для підприємств поділяються на наступні види:

ERP (англ. Enterprise Resource Planning) - система планування (управління) ресурсами підприємства.

CRM (англ. Customer relationship management) - модель взаємодії, що визначає, що центром всієї філософії бізнесу є клієнт, а основними напрямками діяльності є заходи з підтримки ефективного маркетингу, продажів і обслуговування клієнтів.

ECM (англ. Enterprise Content Management) - це стратегічна інфраструктура і технічна архітектура для

підтримки єдиного життєвого циклу неструктурованою інформації (контенту) різних типів і форматів.

CPM (англ. Corporate Performance Management) - концепція управління ефективністю бізнесу, що охоплює весь спектр завдань в області стратегічного і фінансового управління компанією.

HRM (англ. Human Resource Management) - галузь знань і практичної діяльності, спрямована на своєчасне забезпечення організації персоналом і оптимальне його використання.

EAM (англ. Enterprise Asset Management) - це інформаційна система, призначена в основному для автоматизації процесів пов'язаних з технічним обслуговуванням устаткування, його ремонтом, а також післяпродажним обслуговуванням цього обладнання.

Основну загрозу функціонуванню інформаційних систем становлять таргетовані (цільові) атаки.

Особливість цілеспрямованих атак (APT) полягає в тому, що зловмисників цікавить конкретна компанія або державна організація. Це відрізняє дану загрозу від масових хакерських атак - коли одночасно атакується велике число цілей і найменш захищені користувачі стають жертвою. Цілеспрямовані атаки зазвичай добре сплановані і включають кілька етапів - від розвідки і впровадження до знищення слідів присутності. Як правило, в результаті цілеспрямованої атаки зловмисники закріплюються в інфраструктурі жертви і залишаються непоміченими протягом місяців або навіть років - протягом усього цього часу вони мають доступ до всієї корпоративної інформації.

Під інформаційною безпекою слід розуміти захищеність від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації або її власникам. Завдання забезпечення інформаційної безпеки повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Існує багато методів забезпечення інформаційної безпеки:

засоби антивірусного захисту;

засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами;

інструменти перевірки цілісності вмісту дисків;

віртуальні приватні мережі;

міжмережеві екрани;

засоби аутентифікації користувачів;

системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожен з перерахованих методів може бути використаний як самостійно, так і в інтеграції з іншими. Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, та можуть бути видалені. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервери, міжмережеві екрани, що працюють під практично будь-який з поширених операційних систем (Windows, Unix-і Linux системи, Novell).

Для забезпечення криптографічного захисту компанія Eset пропонує використання продукту ESET Endpoint Encryption (EEE).

Важливо зазначити, що в ESET Endpoint Encryption використовується модуль шифрування DESlock.

ESET Endpoint Encryption Server здійснює всі операції з клієнтськими робочими станціями за допомогою консолі DESLock + Enterprise Server. Також користувач має змогу здійснювати операції шифрування безпосередньо на клієнтській робочій станції.

Для забезпечення аутентифікації користувачів в інформаційних системах малих та середніх підприємств компанія Eset пропонує використовувати Eset Secure Authentication.

Принцип дії. ESET Secure Authentication (ESA) додає автентифікацію Two Factor Authentication (2FA) до налаштувань доменів Microsoft Active Directory або локальної мережі. Після цього для входу в систему разом зі звичайним іменем користувача та паролем потрібно буде вводити згенерований одноразовий пароль (OTP). Також може створюватися push-сповіщення, яке має бути підтверджене на мобільному телефоні під керуванням ОС Android, iOS або Windows, коли користувач успішно пройшов автентифікацію за допомогою облікових даних загального доступу.

Для забезпечення безпеки робочих станцій та серверів компанія Eset пропонує використання свого продукту Eset Endpoint Protection, до складу якого входять Eset Endpoint Security (для робочих станцій) та Eset File Security for Windows

Server (для Windows Server) та аналогічні версії програми для інших операційних систем.

ESET Security Management Center (раніше відома як ERA) - це додаток для централізованого управління продуктами ESET на клієнтських робочих станціях, серверах і мобільних пристроях в мережевому середовищі. Завдяки вбудованій в ESET Security Management Center системі управління завданнями можна встановлювати рішення ESET по забезпеченню безпеки на віддалені комп'ютери і швидко реагувати на нові проблеми і загрози.

Саме по собі рішення ESET Security Management Center не забезпечує захист від шкідливого коду. Для захисту середовища потрібно, щоб на робочих станціях було встановлено рішення ESET по забезпеченню безпеки, наприклад ESET Endpoint Security.

Таким чином, правильна реалізація технології захисту інформаційних систем підприємства на базі рішень ESET повинна забезпечити ефективний захист інформаційних ресурсів підприємства та кібербезпеку інформаційної системи підприємства.

Література:

1. FossDoc. Класифікація інформаційних систем [Електронний ресурс] – Режим доступу: https://fossdoc.com/klassifikacija-informacionnyh-sistem

2. Tadviser. Advanced Persistent Threat (APT). Таргетированные или целевые кибератаки. "Развитая устойчивая угроза" 2019/11/25 [Електронний ресурс] – Режим доступу: http://www.tadviser.ru/index.php/Статья:APT_-_Таргетированные_или_целевые_атаки

ПОБУДОВА СУЧАСНОГО ПРОЦЕССУ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Долинний Дмитро Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

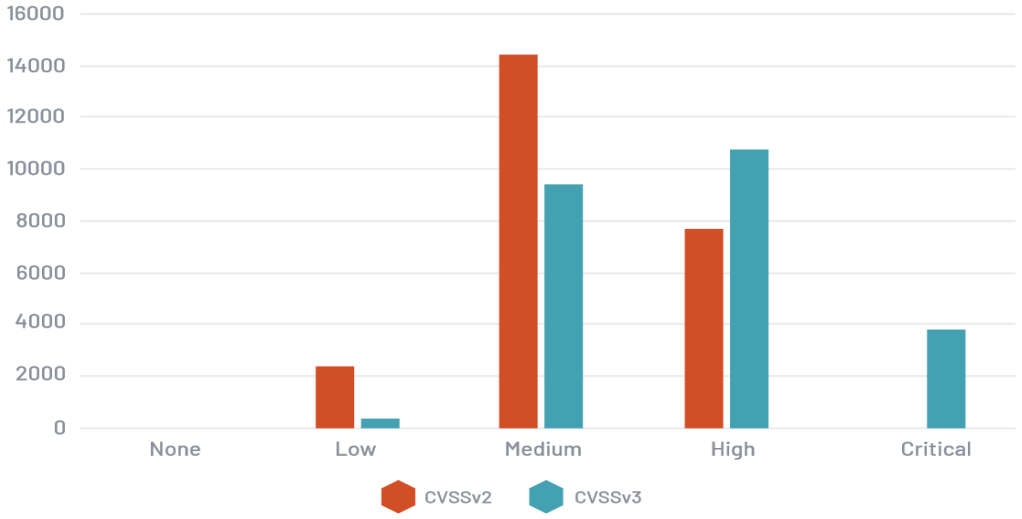
Здійснено аналіз основної моделі процесу управління вразливостями, Розглянуто ряд питань, що стосуються безпосередньо захисту інформаційних систем. Зокрема, яким чином діяльність узгоджується із загальноприйнятими уявленнями про реалізацію процесу управління вразливостями. Визначено актуальність дослідження та вказано на основні проблеми в сфері захисту від кібератак.

На сьогоднішній день, більшість компаній не до кінця розуміють існуючі ризики в їх інфраструктурі та мережі. Більшість компаній продовжують закривати вразливості

опираючись на загальноприйнятий застарілий підхід, беручи до уваги лише оцінку CVSS. Як показує практика 2017 року, коли віруси шифрувальники експлуатували вразливість, яка на той час мала оцінку меншу за 6.0, хоча завдала колосальних збитків, цей метод не є актуальним.

Незалежно від того, як давно ви перебуваєте в кібербезпеці, ви знаєте, що управління вразливостями має важливе значення для виявлення та зменшення кібер-ризику. Чому? Оскільки за кожною головною кібератакою стоїть вразливість, яка залишилась без розгляду. Але є одна велика проблема: за останні 20 років поверхня атаки еволюціонувала, і управління вразливостями не встигало за цим. Сьогодні IT-середовище постійно змінюється. Рухаючись цифровою трансформацією, наш світ тепер написаний кодом, вируючи новими технологіями, платформами та пристроями. Подумайте про хмарні, IoT, мобільні, веб-програми, навіть промислове обладнання підключається до цього хаотичного ландшафту. Різні типи активів постійно надходять і виходять з підприємства. На додачу до цього, деякі є ефемерними - тривають лише секунди або хвилини.

Враховуючи поверхню аеростатичної атаки, не дивно, що кількість вразливостей зростає. Насправді, підрахунок просто відлякує. З 2016 по 2018 рік нові опубліковані вразливості зросли з 9 8372 до 16 500 на рік. В середньому це означає, що підприємства знаходять 870 вразливостей на день у 960 IT-активах. Додаючи до виклику, ступінь серйозності вразливості зростає. Через зміни, внесені до загальновизнаної системи оцінки вразливості (CVSS), більшість вразливостей зараз класифікуються як високі або критичні. Згідно з рейтингами CVSSv3, 60% вразливостей вважаються високими або критичними порівняно з 31% у CVSSv2 (див. Таблиця 1).



Таблиця 1. Зрівняння оцінки CVSSv2 та CVSSv3

В результаті команди безпеки стикаються з більшою кількістю вразливостей, ніж вони можуть впоратись. Поширення цих обмежених і цінних ресурсів може швидко призвести до неефективності та вигорання роботи. І оскільки CVSS, по суті, не усвідомлює ризиків, останнє, що вам потрібно, це витратити дорогоцінний час на виправлення вразливих місць, які не несуть великий ризик.

Усі знають, що немає жодних гарантій від порушення безпеки. І найкраще рішення, яке може прийняти організація- управління вразливостями на основі ризиків. За допомогою цього методу ви повинні впевнено відповісти на три ключові питання:

1. Які вразливості знаходяться в інфраструктурі?

2. Де нам слід визначити пріоритети на основі вірогідності експлуатації?

3. Який вплив буде на організацію при експлуатації вразливості?

Управління вразливістю на основі ризиків допомагає вирішити величезний обсяг питань пов'язаних з вразливостями, надаючи точну увагу дійсно актуальним вразливостям, щоб діяти швидко та ефективно.

Спочатку вирішіть фундаментальну проблему- що знаходиться у вас в інфраструктурі?

1. Встановити автоматизовані сканери.

2. Провести інвентаризацію обладнання.

3. Визначити слабкі місця в інфраструктурі.

4. Пріоритизувати пристрої на яких впершу чергу повинні бути закриті вразливості.

5. Впровадити механізм, який основується на алгоритми машинного навчання, який аналізує різні джерела(dark net, форуми, минулі атаки, час коли останній раз була виявлена експлуатація вразливості і тд. і тп) для пріоритизації дійсно актуальних вразливостей, які несуть ризик.

6. Усунути вразливості.

7. Провести аналіз сформованої інфраструктури.

За допомогою управління вразливістю на основі ризику ви отримаєте необхідну інформацію для захисту бізнес-систем. Якщо кібер-ризик бізнес-системи недопустимий, ви можете швидко визначити, куди зосередити додаткові засоби контролю для зменшення ризику. Ви також зможете легко повідомити кібер-ризик своєї інфраструктури керівникам підприємств. Дані, на які ви покладаєтесь для ефективного визначення та управління вашим рішенням по управлінню вразливостями,

автоматично вкладаються в метрику, засновану на оцінці ризику, яку зрозуміють власники бізнесу.

Література:
Computer Security Incident Handling Guide//https://csrc.nist.gov/publications/detail/sp/800-61/archive/2004-01-16

ВИКОРИСТАННЯ ВІДДАЛЕНИХ КОЛЕКТОРІВ ЛОГІВ В СУЧАСНИХ СИСТЕМАХ ЗАХИСТУ ВЕБ-ДОДАТКІВ

Дорохін Орест Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Описані проблеми забезпечення надійного зберігання логів для швидкого й безперебійного доступу до інформації що є критично важливою для розслідування інцидентів та анадізу роботи систем захисту веб-додатків, таких як WAF (Web Application Firewall) та ін.. З метою демонстрації задіяно такі продукти, як Elastic Stack та F5 AWF (Advanced Web Application Firewall). Розглянуто шляхи вирішення даного питання через використання віддалених колекторів логів.

На захищеність веб-додатків компанії наразі впливає безліч факторів й ринок засобів захисту пропонує безліч рішень: це системи запобігання вторгнень Intrusion Prevention System (IPS), антивіруси, системи моніторингу «сирого» та сегментованого трафіку, системи Security Information and Event Management (SIEM), брандмауери типу Next Generation Firewall (NGFW), системи запобігання витоку даних Data Leak Prevention (DLP) й багато інших. Побудова захищеної інфраструктури для роботи веб-сервісів вимагає високої кваліфікації спеціалістів та часу на розгортання й налагодження, настільки, що в сучасних реаліях часто переходять на делегування захисту віддаленим SOC (Security Operation Center). Логи та події, їх збір та аналіз є невід'ємним завданням при розслідуванні інцидентів, а їх форма та доступність грають вирішальну роль в умовах необхідності негайної реакції. В даній роботі розглянуто шляхи вирішення питання забезпечення надійного зберігання та доступу до логів та подій що генеруються WAF на прикладі технологій F5 Networks та Elastic Stack.

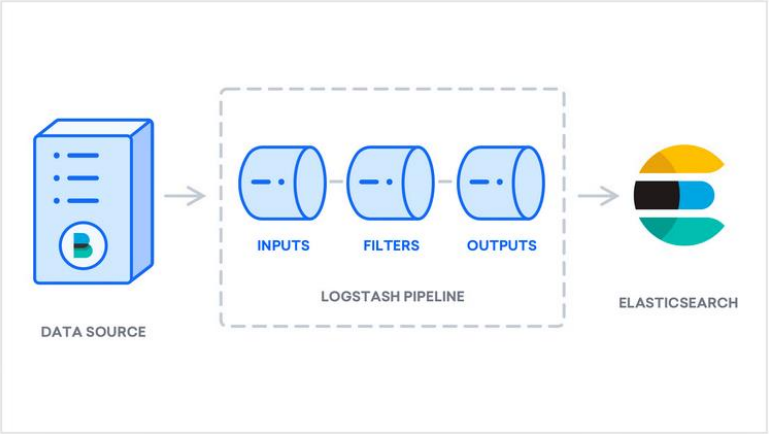


Рис. 1 Етапи обробки трафіку від джерела даних до Elasticsearch

Локальне зберігання логів може вплинути на продуктивність диска, особливо з повільними дисковими підсистемами. Великі об’єми подій безпеки вимагають постійної їх ротації на диску, що також навантажує CPU та RAM, віднімаючи ресурси з плану профільних завдань WAF. Не кожен WAF може відобразити атаки й побудувати комплексні візуальні графіки по обробленому трафіку настільки якісно як це зробить профільна система. Elastic Stack може виступати основою SIEM-системи адже вирішує дані питання. Компанія F5 Networks, що наразі займається розробкою й підтримкою NGINX, рекомендує надсилати логи й події безпеки на віддалені SIEM для кращого збереження даних, пошуку, кореляції подій та масштабованості [1].

В F5 Adwanced Web Application Firewall (AWF) для відправлення логів та подій на віддалені сховища використовуються протоколи TCP та UDP. UDP компактніший, але може реєструвати лише до 1 КБ даних на запис журналу, тоді як TCP забезпечує більшу надійність і дозволяє до 64 КБ даних на запис журналу. Така більша ємність даних робить TCP кращим вибором, оскільки дозволяє зберігати цілі записи в журналі. F5 рекомендує використовувати логування сесій лише для порушень, а не всіх запитів.

«ELK stack» - це скорочення від трьох проектів з відкритим вихідним кодом: Elasticsearch, Logstash і Kibana. Розробляється компанією Elastic разом з усіма пов'язаними проектами. Elasticsearch - це ядро всієї системи, яка поєднує в собі функції бази даних, пошукової та аналітичної системи. Logstash - це конвеєр обробки даних на стороні сервера, який отримує дані з декількох джерел одночасно, парсит лог, а потім відправляє в базу даних Elasticsearch. Kibana дозволяє користувачам візуалізувати дані за допомогою діаграм і графіків

в Elasticsearch. Також через Kibana можна адмініструвати базу даних.

Формати даних, які F5 AWF може використовувати для передачі SIEM:

- Comma-Separated Values
- Key-Value Pairs
- Common Event Format (ArcSight)
- F5 BIG-IQ Centralized Management

Дані з F5 в ELK передано, використовуючи формат «Key-Value Pairs».

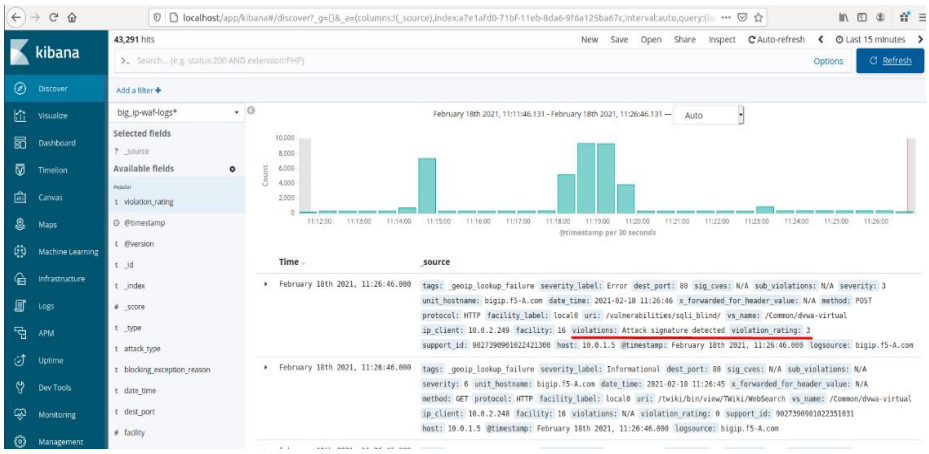


Рис. 1 Реєстрація атаки й відображення її в Kibana

Література:

1. BIG-IP ASM operations guide | Chapter 3: BIG-IP ASM event logging [Електронний ресурс] – Режим доступу : World Wide Web. – URL: https://support.f5.com/csp/article/K37655278

ЩОДО НЕОБХІДНОСТІ ВИКОРИСТАННЯ ТАКТИК ПОРУШНИКІВ ДЛЯ ПОКРАЩЕННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Драгунцов Роман Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Особливістю сучасного ландшафту загроз інформації є розповсюдженість складних таргетованих атак, що залучають або ще невідомі тактики, або такі, що є складно формалізованими. Успішність таких атак може призводити до серйозного впливу на інформаційні системи цільової організації. Існуючі засоби сигнатурного захисту, системи виявлення та попередження вторгнень, тощо, часто виявляються не ефективними самі по собі для виявлення та зупинення таких загроз [1]. Саме тому існує необхідність у нелінійному виявленні та відповіді на основі аналізу поведінки.

Дана задача може вирішуватись за допомогою штучного інтелекту або залучення відповідного персоналу – використання відповідних операційних центрів. Проблема практичної підготовки кадрів з числа персоналу вище згаданих операційних центрів постає особливо актуальною. Можливість виявлення аномалій у функціонуванні мережі може грунтуватись лише на досвіді – порівнянні звичайного режиму функціонування системи з аномальним на основі кореляції багатьох джерел інформації. Так чи інакше, існує необхідність вивчення та використання тактик зловмисників для створення відповідного досвіду [2].

Використання тактик, що вже були виявлені в реальних умовах, в процесі тестування захищеності інформаційних систем дозволяє отримати позитивний результат для стану безпеки: з одного боку, відбувається виявлення конкретних недоліків та вразливостей безпеки для подальшого усунення; з іншого, персонал інформаційної безпеки в ході здійснення моніторингу активності в інформаційній системі може визначати неочевидні ознаки проведення атаки, ідентифікатори компрометації та інші факти, що дозволяють виявляти порушення. Такий досвід дозволяє персоналу безпеки створювати більш ефективні кореляційні правила та сценарії (playbook), для використання під час роботи операційного центру, а також в особистому порядку більш ефективно виявляти небезпечні аномалії у функціонуванні інформаційної системи.

Перспективним напрямком дослідження є розробка конкретних методів та процесів взаємодії спеціалістів з тактик порушників та спеціалістів захисту та механізмів, що можуть бути використані для створення відповідних правил автоматизації.

Література:

1. Global Threat Report [Електронний ресурс] / Crowdstrike – 2018. – Режим доступу до ресурсу: https://www.africacybersecurityconference.com/document/CrowdStrike_GTR_201 9.pdf

2. Blue-team vs. Red-team Tabletop Exercise to Train the Process of Attack Investigation [Електронний ресурс] / [Y. Masuda, C. Matsuda, Y. Kon та ін.] // 31st Annual FIRST conference. – 2019. – Режим доступу до ресурсу: https://www.first.org/resources/papers/conf2019/Blue-team-vs.-Red-team-Tabletop-Exercise-to-Train-the-Process-of-Attack-Investigation.pdf.

ЗАСОБИ ТА ПРАВИЛА ЗАХИСТУ ПІДПРИЄМСТВА ТА ІНФРАСТРУКТУР ВІД КІБЕРАТАК

Дріга Станіслав Сергійович
Державний університет телекомунікацій

Навчально-науковий інститут Захисту інформації
м. Київ

В роки розвитку кіберпростору і комп'ютерних технологій дуже стрімко розвиваються технології і з цим підвищується рівень технологічної небезпеки на підприємствах. Чим більше технологій буде впроваджено, тим ретельніше треба за ними слідкувати та позбавлятись кожної вразливості. Для усього цього були розроблені правила поведінки у комп'ютерних системах. Правила з заощадження інформаційної безпеки.

У сучасний час інтенсивного розвитку інформаційних технологій зростає проблема підвищення рівня захисту інформації. Тому актуальність впровадження та вдосконалення технологій безпеки інформаційних систем існує зараз і буде існувати надалі.

Сучасні інфраструктури та різні корпоративні і інформаційні системи дуже тісно пов'язані з інформаційними технологіями. Інформаційна безпека у таких випадках невід'ємний елемент IT-структур. Будь яка організація має правильно забезпечити збереження усіх своїх даних та їх конфіденційність. Найбільш важливими для захисту є підприємства галузей, як банки, енергетична та хімічна промисловість, телекомунікаційні установи або охорона здоров'я. Ці установи є стратегічно важливими для економіки та безпеки держави тому їх називають критично важливими об'єктами інфраструктури. Такі об'єкти найбільш схильні до атак кібертерористів та хакерів. Європейський Союз визначає критичну інфраструктуру як системи, які мають важливе значення для підтримки життєво важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисного поведінки, може істотно негативно вплинути на безпеку ЄС і добробут громадян. [1], [2]

Кожна компанія чи установа повинна впроваджувати політику інформаційної безпеки. Це правила котрі повинні працювати в організації для управління та захисту критичної інформації. Такі правила мають бути задокументованими та мають описувати у собі практичні прийоми та керівничі принципи галузі безпеки інформації якими буде керуватись організація.

У таких правилах розглядаються такі напрямки, як:

- Захист програм обробки інформації;
- Захист різних каналів зв'язку передачі інформації;
- Контроль над системою захисту;
- Запобігання електромагнітних випромінювань і наведень;
- Забезпечення захисту об'єктів ІС;

Для проведення такої політики завжди описуються різні етапи створення системи захисту. Це надає змоги зрозуміти, що саме треба захистити і яким чином. Для початку треба визначити які інформаційні та технічні ресурси підлягають захисту. Потім повністю виявити потенційні загрози та канали витоку інформації. Це надає змоги провести оцінку вразливостей та ризиків втрати інформації. Після оцінки організація визначається з вимогами до системи захисту даних та здійснює вибір засобів захисту інформації та впровадження їх в систему. Та надання контролю керування системою захисту спеціалістам з технічного захисту інформації.

Документи політики ІБ завжди поділяють за рівнями захисту. Такі рівні зазначені у стандарті **ISO / MEC 17799-2005. Це міжнародний стандарт згідно якому на верхньому рівні політики ІБ повинні оформлюватись документи такі як «Концепція забезпечення Інформаційної Безпеки», «Правила використання ресурсів інформаційної безпеки» та «План забезпечення безперервності бізнесу».**

У середній рівень входять документи які керують окремі аспекти інформаційної безпеки. До них входять різні вимоги експлуатації захисту інформації та організацію інформаційних процесів у конкретних напрямках захисту таких як: Комунікаційна безпека, використання різних засобів інформації, робота з криптографічними системами. Такі документи завжди є внутрішніми стандартами організації та повинні бути повністю конфіденційними.

До нижнього рівня політики ІБ входять вже регламент робіт, проведення адміністрування системи та впровадження інструкцій з експлуатації використаних сервісів захисту інформації які використовує установа.

Засоби захисту інформації діляться на організаційний захист та програмно технічний.

Організаційний захист - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ. [3]

Сюди входять:

- Організація системи охорони, мета якої урегулювання захисту території, та виключення можливості проникнення сторонніх осіб на територію підприємства;

- Організації регулювання співробітників. Надання правил роботи з інформацією та заходів відповідальності за прошення правил захисту ІБ;
- Організація проведення технічних засобів обробки та зберігання конфіденційної інформації;
- Робота та аналіз над виявленням зовнішніх та внутрішніх загроз витоку інформації та заходів щодо її захисту;
- Ведення обліку персоналу, контроль їх роботи з конфіденційною інформацією.

До програмно-технічного захисту інформації входять декілька видів та підвидів захисту. Наприклад існують засоби захисту від несанкціонованого доступу до інформації. До нього входять:

- Авторизація персоналу;
- Мандатне управління;
- Виборче управління доступом;
- Надання різних прав персоналу;
- Ведення аудиту або журналу системи захисту.

Також існують різні системи аналізу та моніторингу мереж до якої може входити різноманітні програми, системи виявлення вторгнень та способи їх запобігання. Також перевірка на виток конфіденційної інформації.

Окрім цього в систему можуть бути впровадженні різні антивірусні системи, мережеві екрани захисту, криптографічні засоби такі як цифровий підпис та шифрування даних. Розробка резервного копіювання даних, джерел безперебійного живлення та генератори електроживлення.

Співробітники технічної безпеки повинні також розробити систему аутентифікації персоналу. Завдяки впровадженню паролів, ключів доступу, різноманітних сертифікатів та біометричних даних.

Література:

1. European Programme for Critical Infrastructure Protection (EPCIP) [online] - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260

2. European Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

3. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96 [online] - http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38911&cat_id=38836

ЗАХИСТ ІНФОРМАЦІЇ В ВЕБ-ЗАСТОСУНКАХ

Євсеєв Дмитро Сергійович, Сіроштан Юлія Олександрівна
Харківський національний економічний університет

ім. Семена Кузнеця
м. Харків

Стрімке зростання глобальної мережі Інтернет та розвиток інформаційних технологій привели до формування інформаційного середовища, яке безпосередньо впливає на сфери людської діяльності. Нові технологічні можливості значно полегшують обмін інформацією, її пошук та зберігання, що у свою чергу потребує чіткого розуміння захисту інформації та даних які зберігаються на веб-сервісах. Нормою сьогодні є спілкування за допомогою мережі, електронний документообіг та залучення "хмарних" ресурсів для різного роду інформаційних потреб підприємств та окремих користувачів. У зв'язку з цим загострилися питання безпеки інформаційних ресурсів за всіма її складовими: кібербезпеки та інформаційної безпеки. Основними механізмами забезпечення основних послуг безпеки – конфіденційності, цілісності та автентичності, є шифрування, цифровий підпис та автентичність.

Враховуючи відмінність завдань і методів побудови сайтів, вони мають різні критерії їх оцінювання. На першому рівні розробки веб-сервісів головна увага приділяється зручності та адаптації користувача до інтерфейсу, на другому рівні потрібно створити структурну складову зі усіма функціональними можливостями сервісу, та останнє з головних пунктів, являється захист інформаційної та функціональної складової веб-застосунку. Компанії, які використовують веб-сервіси для оптимізації роботи і залучення нових клієнтів, зростає щорічно. Без будь-яких сумнівів, веб-сервіси несуть величезну кількість переваг, з іншого боку – при збільшенні кількості додатків також зростає і кількість кіберзагроз. За статистикою звіту Global Internet Security Threat Report (ISTR), яка надала компанія Symantec вказуючи на три поширених злому: за допомогою вразливості веб-сервісу на сервері; за допомогою комп'ютерної програми (експлойт) для пошуку вразливостей операційної системи; за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію. У зв'язку зі збільшенням кібератак виникла потреба для оновлення старих методів захисту та створення нових. Для запобігання взлому вразливостей системи веб-сервісу, потрібно визначити проблеми безпеки, перш ніж зловмисник ідентифікує і використовує їх. Існує певна кількість варіантів захисту: дуже важливо регулярно виконувати процес виявлення вразливостей веб-додатку на протязі життєвого циклу розробки програмного забезпечення (SDLC), а не тільки в процесі експлуатації; тестування на ранніх стадіях розробки має першорядне

значення, оскільки в подальшому може бути дуже складно або зовсім неможливо забезпечити безпеку додатку, не переписавши його. Чим раніше безпеку веб-додатки буде включена в проект (by design), тим більш безпечним буде веб-додаток і тим дешевше і простіше буде усунути виявлені проблеми на більш пізньому етапі. Існує кілька технологій виявлення вразливостей в веб-додатках: автоматичне сканування за принципом білого ящика (white box); перевірка вихідного коду вручну; тест на проникнення (penetration test); автоматичне сканування за принципом чорного ящика (black box). В рамках наукового дослідження планується провести оцінку сучасних методів захисту інформації веб-сервісів. Враховуючи збільшення кількості кібератак з кожним роком, потрібно проявити більшу увагу даним методам, які можуть допомогти з безпекою конфіденційних даних бізнесу та веб-сервісів.

Література:

1. Кібербезпека: Лабораторний практикум з основ криптографічного захисту // С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.

2. Cybersecurity Essentials [Електронний ресурс] // cisco networking academy. – 2020. – Режим доступу до ресурсу: https://lms.netacad.com/course/view.php?id=2245.

3. Суханов А. Захист даних веб-додатків від внутрішніх загроз [Електронний ресурс] / Александр Суханов // Anti-Malware.ru. – 2018. – Режим доступу до ресурсу: https://www.anti-malware.ru/practice/solutions/web-applications-internal-threats-security.

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У ЗВ'ЯЗКУ З ПАНДЕМІЄЮ COVID-19

Завадський Володимир В'ячеславович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Проблеми кібербезпеки станом на 2020 рік стали ще більш актуальними, як ніколи. Кожного дня люди все більше починають стикатись з використанням Інтернету у повсякденному житті. Причиною цього є перехід на дистанційні методи зв'язку через пандемію Covid-19.

Ключові слова: кібербезпека, пандемія, опитування, covid-19.

За даними ISSA [1] та EGS [2], кіберзлочинці збільшили атаки, пов'язані з пандемією на 63%. Статистично 39% респондентів стверджували, що були повністю готовими до такого зросту, навпроти 27% опитуваних були повністю беззбройними проти такого натиску. Також можна зазначити, що 38% компаній покращили зв'язки з службами кібернетичної безпеки.

Лише 20 відсотків вважають, що вимоги безпеки COVID-19 призведуть до збільшення витрат на безпеку в 2020 році, тоді

як 25 відсотків вважають, що їх організації будуть змушені зменшити витрати на безпеку цього року. Там, де вони очікують збільшення своїх витрат, принаймні наполовину вказували на пріоритетні сфери - управління ідентифікацією та доступом, безпеку кінцевих точок, web безпеку та електронної пошти та безпеку даних.

Нарешті, чи викликає COVID-19 фахівців з кібербезпеки стурбованість своєю роботою чи вибором професії? Загалом, відповідь на обидва питання, як видається, "ні", однак, схоже, дані вказують на те, що в короткостроковій перспективі існує більша невизначеність щодо поточних робочих місць у галузі кібербезпеки.

«COVID-19 мав широкий вплив на людей на співробітників служби безпеки. Оскільки 84 відсотки фахівців з кібербезпеки працювали виключно з дому під час пандемії, і майже дві третини вважали, що їх організації будуть більш гнучкими, застосовуючи політику роботи вдома, COVID-19 особисто вплинув на фахівців з кібербезпеки на своїх робочих місцях та в повсякденному житті. До цього ж, щорічно погіршується проблеми дефіциту навичок кібербезпеки», - Джон Ольцік, старший головний аналітик та науковий співробітник ESG [2].

«Хоча багатообіцяюче бачити, що більшість організацій змогли досить добре впоратися з пандемією COVID-19, дивно, що ми не спостерігаємо збільшення витрат на кібербезпеку або встановлення пріоритетів після цієї події. У будь-якому випадку це повинно послужити сигналом пробудження, що кібербезпека - це те, що дозволяє компаніям залишатися відкритими та функціонувати. Організації, які надають пріоритет кібербезпеці в результаті пандемії, швидше за все, стануть лідерами в наступній хвилі інновацій та найкращих практик процесу кібербезпеки», - сказала Кенді Олександр, президент правління ISSA International [1].

Отже, викладені зміни торкнуться не лише IT-відділу. Якщо віддалені співробітники продемонструють, що працюють ефективніше вдома, менеджерам по роботі з кадрами доведеться переглянути свою політику, щоб забезпечити кращий баланс між роботою та особистим життям. Тим часом людей з критичними навичками та вимогами до віддаленої роботи потрібно буде швидко знаходити та ефективно використовувати. Крім того, великі корпорації стикаються з новими обмеженнями щодо бюджету. З’являться нові способи використання коштів та інвестування у правильні позиції. Фірми будуть суворіше розподіляти ресурси.

Література:
1. *https://ww1.issa.int/*
2. *https://www.esg-global.com/*

5 ТРЕНДІВ, ЯКІ ЗМІНЯТЬ ТЕЛЕКОМУНІКАЦІЇ В 2021 РОЦІ

Завадський Володимир В'ячеславович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Ми наближаємося до кінця 2020 року і початку нового десятиліття, в якому ми очікуємо приголомшливі можливості технологічних інновацій. За останні кілька років ми стали свідками неодноразових звітів про тенденції, в яких багато говорилося про 5G, хмарні сервіси, блокчейн, периферійні обчислення, IoT і т.д.

Я обрав 5 тенденцій:

1. **5G для всіх**

Вірно, що ми повторюємося. Про 5G [2] говорили, говорять і будуть говорити на багатьох форумах. Однак все це зміниться в 2021 році. Технологія вже існує, але не є широко доступною в якості послуги на ринку для користувачів. У наступаючому році оператори зможуть пропонувати мережі 5G і їх удосконалення, що забезпечують більшу пропускну здатність, більш високу щільність користувачів, низьку затримку і надійність.

Якщо на мить зосередитися на Іспанії, ми побачимо, що Vodafone вже розгорнув мережу 5G, Telefonica планує розгорнути 5G в автономному режимі (NSA) до кінця 2020 року, а Orange вирішила почати роботу в режимі SA в 2021 році.

Я повинен згадати тут, що 5G - це не тільки збільшення пропускної здатності, а й надання додаткових послуг для мільярдів взаємопов'язаних пристроїв, які обмінюються або відправляють інформацію в центри управління для прийняття рішень. Компанії, уряд і клієнти виграють від повного зв'язку, а установам необхідно співпрацювати один з одним, щоб сприяти цьому прогресу. Наприклад, ЄС планує до 2025 року забезпечити безперебійне покриття 5G для залізних і основних доріг.

2. **Супершвидкий Wi-Fi 6.**

Провідні виробники вже представили Wi-Fi 6 [1] - також відомий як 802.11ax - в своїх портфоліо продуктів. Але з відкриттям офіційної програми сертифікації Wi-Fi Alliance

очікується, що в 2021 році більше постачальників послуг офіційно і широко розгорнуть цю технологію.

5G і Wi-Fi 6 - це абсолютно різні технології, які можуть конкурувати в багатьох високошвидкісних сценаріях без використання кабелю. Але насправді ці дві технології, які працюють разом, являють собою ідеальну комбінацію наскрізного підключення для дому та офісу.

Wi-Fi 6, як і 5G проти 4G, не тільки має на увазі теоретично більш швидку передачу даних, але і вирішує деякі проблеми, присутні в попередніх мережах, такі як щільність підключених терміналів і низька продуктивність мережі при збільшенні цієї щільності.

Очікується, що кількість мережевих пристроїв Wi-Fi буде рости дуже високими темпами. Мало того, споживання даних і можливості мережевого інтелекту також повинні рости, щоб йти в ногу з вимогами кінцевих користувачів до послуг і якості.

3. **Штучний інтелект (AI) і великі дані**

Сектор телекомунікацій розглядає штучний інтелект [3] - як засіб значного поліпшення комунікаційних технологій і послуг. Щоб оптимізувати свої операції, оператори впроваджують штучний інтелект, щоб пропонувати поліпшені сервіси для клієнтів, створювати більш розумні реалізації мереж і створювати нові компанії, які можуть розробляти більш просунуті послуги.

AI все частіше використовується в різних сферах діяльності компаній. Це важливо для оптимізації і профілактичного обслуговування мереж телекомунікаційних компаній. AI використовує чат-ботів і віртуальних помічників, щоб поліпшити обслуговування клієнтів і підвищити їх задоволеність. З'являється все більше і більше продуктів, пов'язаних з AI, для виявлення шахрайства. І якщо цього було недостатньо, AI полегшує прийняття і виконання рішень на основі аналізу великих обсягів даних, що збираються кожен день з кількох джерел.

4. **Інтернет речей (IoT)**

Розширення нових технологій зв'язку, описаних вище, дозволить в 2021 році підключати багато повсякденних пристроїв один до одного і до Інтернету. Багато з цих пристроїв уже існують сьогодні, але не дуже інтелектуальні і працюють автономно. Інтернет речей дозволить поліпшити обмін інформацією, моніторинг базових станцій, збір даних вимірювань, віддалене управління і автоматизоване прийняття рішень.

Інтернет речей зможе використовувати такі комунікаційні технології, як BLE, 5G або Wi-Fi 6. Але Інтернет речей включає не тільки технології підключення; це також чудова можливість для створення нових послуг для промисловості та інших секторів ринку.

Інтернет речей привів до появи все більшої кількості пристроїв в мережі, а також до збільшення можливостей для порушень безпеки. Керівники постачальників цих нових послуг і технологій повинні спланувати способи захисту конфіденційності даних, захисту користувачів від атак і (насамперед) забезпечення надійності. В іншому випадку кінцеві клієнти навряд чи будуть наймати нові послуги, які продаються.

5. **Цифрова конфіденційність, кібербезпека і стійкість**

Взагалі кажучи, цифрова конфіденційність відноситься до рівня контролю, який користувач Інтернету може здійснювати над своїми даними, обмежуючи доступ інших людей або установ до приватної інформації. Конфіденційність настільки важлива для успіху сервісів в загальнодоступних мережах, що в 2019 році ЄС змінив свої вимоги до захисту даних - GRDP.

В (імовірно) більш взаємопов'язаному світі 2021 року кібербезпека матиме ключове значення для того, щоб допомогти компаніям і приватним особам бути менш схильними до ризиків, які можуть завдати великої шкоди. Рішення, орієнтовані на захист, повинні стати невід'ємною частиною нових послуг, пропонованих постачальниками в наступному році.

Нарешті, з огляду на зростаючий ризик, в 2021 році компаніям необхідно буде інвестувати в продукти, які захищають їх від вразливостей і дозволяють їм управляти існуючими ризиками з мінімальним впливом.

Література:

1. *https://ru.wikipedia.org/wiki/IEEE_802.11ax*
2. *https://uk.wikipedia.org/wiki/5G*
3. *https://en.wikipedia.org/wiki/Artificial_intelligence*

БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ. ПРОТОКОЛ HTTP

Колосюк Назарій Геннадійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Розглянуто тему передачі даних, переваги та недоліки в використанні протоколу HTTP. Відмінність в використанні протоколу HTTP і протоколу HTTPS.

Протокол HTTP не передбачає жодних механізмів захисту даних користувача і веб-серверів, якщо не брати до уваги базової схеми аутентифікації клієнтів на сервері, кодування інформації та положень безпеки в стандарті HTTP 1.1. Хоча, дотримуючись рекомендацій безпеки HTTP протоколу, розробники можуть розробляти свої додатки з великим рівнем захищеності. Розглянімо положення про безпеку HTTP протоколу.

Самий істотний недолік базової аутентифікації на сервері, і в той же час найбільший пролом в безпеці HTTP сервера полягає в тому, що логін і пароль користувача передається в HTTP повідомленні в незашифрованому вигляді, тому варто використовувати додаткові методи шифрування при використання базової аутентифікації.

Пролом в безпеці не обмежується тим, що хтось може перехопити HTTP запити або HTTP відповіді з незашифрованими даними, але і в тому, що користувач може замість бажаного ресурсу потрапити на шкідливий клон, в якому він пройде аутентифікацію, тим самим залишивши свої дані зловмисникові.

Сервер може повертати клієнту повідомлення з кодом стану 401 (код помилки клієнта, який говорить про те, що він не авторизований), і разом з кодом помилки 401 сервер може відправити список методів аутентифікації в тому порядку, в якому налаштує адміністратор, зазвичай в порядку зменшення безпеки, для цього сервер використовує поле заголовку www-Authenticate.

Сервер зазвичай записує в спеціальний файл всі запити користувача і відповіді на них, тобто веде лог. На деяких сайтах лог запитів може представляти інтерес для зловмисників. Тому реалізатори серверів повинні подбати про безпеку HTTP запитів.

Протокол HTTP - універсальний протокол передачі даних, а це значить, що з даного протоколу можна передавати, в принципі, будь-яку інформацію. Так само у HTTP протоколу немає ніяких засобів або механізмів, які могли б відрегулювати вміст HTTP повідомлення (HTTP об'єкт). Власне, надсилання даних і безпека передачі даних лежить на клієнтському і серверному програмному забезпеченні, тому до небезпечних полів заголовка HTTP повідомлення можна віднести: Server, Via, Referer, From. Так як вони можуть допомогти ідентифікувати назву і версії програм і, відповідно, скористатися багами цих програм, а також за цими полями можна дізнатися URI (URI в HTTP), на які заходив користувач (URI, до речі, може бути приватним), або дізнатися його контактні дані.

Література:
1. *https://zametkinapolyah.ru*
2. *https://uk.wikipedia.org*
3. *https://habr.com*

ADVANTAGE – НОВИЙ 5000-КУБІТНИЙ КВАНТОВИЙ КОМП'ЮТЕР КОМПАНІЇ D-WAVE

Костроміна Марія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

D-Wave Systems, Inc. — компанія з виробництва квантових комп'ютерів. Квантові комп'ютер (КК) - це обчислювальний пристрій, який використовує явища квантової механіки для передачі і обробки даних. Основна відмінність квантового комп'ютера від класичного полягає в поданні інформації. Робота квантового комп'ютера грунтується на принципі суперпозиції, а замість бітів використовуються квантові біти, іменовані кубитами. У кубіта також є два основні стани: нуль і одиниця. Однак завдяки суперпозиції кубіт може приймати значення, отримані шляхом їх комбінування, і перебувати у всіх цих станах одночасно. У цьому полягає паралельність квантових обчислень, тобто відсутність необхідності перебирати всі можливі варіанти станів системи.

Не так давно представники відомої канадської компанії D-Wave оголосили про розробку нової квантової обчислювальної системи, призначеної вже виключно для комерційного використання. Ця система, що отримала назву Advantage, містить 5 тисяч кубітів, кожний з яких володіє 15 варіантами з'єднань з іншими кубітами. І новий квантовий комп'ютер буде доступний для корпоративних клієнтів через Інтернет і хмарний сервіс під назвою "Leap Quantum".

Протягом декількох останніх років деякі відомі технологічні компанії приділили достатньо велику увагу питанням розробки істинного квантового комп'ютера, який може вирішувати найскладніші завдання, недоступні для вирішення звичайними комп'ютерами. Прогрес в цій області рухається дуже повільним темпом, особливо якщо порівнювати його з темпами прогресу розробок перших звичайних комп'ютерів.

Такі компанії, як Google і IBM, працюють над класичної квантової архітектурою, в якій кубіти, точніше їх стан, змінюється в міру виконання квантового алгоритму. На відміну від цього, компанія D-Wave спочатку була націлена на реалізацію технології так званого квантового відпалу, в якій все будується на охолодженні кубітів під час виконання алгоритму,

що призводить до пасивного зміни значення міститься в них квантової інформації.

Порівняння архітектури класичного квантового комп'ютера і архітектури комп'ютерів компанії D-Wave не має ніякого сенсу через їх функціональних відмінностей. Тому наявність в системі Advantage 5 тисяч кубітів не обов'язково означає безумовного переваги перед класичними системами з сотнею кубітів, які зараз вже створені іншими компаніями. Однак, квантові системи компанії D-Wave, незважаючи на їх деякі очевидні недоліки, вже прямо зараз можна використовувати для вирішення практичних завдань.

Представники компанії D-Wave відзначають, що безліч клієнтів використовували їх системи для вирішення власних завдань. Компанія AI Menten проектувала і моделювала на квантовому комп'ютері нові білки, мережа магазинів Save-On-Foods використовувала його для оптимізації логістики та інших ділових операцій, а Volkswagen - для створення нової більш ефективної системи фарбування автомобілів і т.п.

Крім системи із збільшеною кількістю кубітів і варіантів їх сполуки, клієнти компанії D-Wave отримають в своє розпорядження гнучкий доступ до системи, розширений набір гібридних програмних інструментів і програмного забезпечення, і, природно, до оновлень системи, які будуть випускатися пізніше.

Крім цього, фахівці D-Wave аналізуватимуть специфіку розв'язуваних на їх новій системі завдань, плюс отримувати зворотний зв'язок від користувачів, що дозволить їм в майбутньому розширити функціональність системи і зробити квантові обчислення доступними більш широкому колу потенційних клієнтів.

Література:

1. *https://www.dwavesys.com/*
2. *https://blog.allo.ua/kvantovye-kompyutery_2018-07-39/*
3. *https://www.dailytechinfo.org/infotech/10968-advantage-novyy-5000-kubitovyy-kvantovyy-kompyuter-kompanii-d-wave.html*

ПОВНІСТЮ РОБОТИЗОВАНА ХІМІЧНА ЛАБОРАТОРІЯ ПІД УПРАВЛІННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Костроміна Марія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Інтелектуальна лабораторія, здатна самостійно планувати і проводити експерименти з області квантової фізики. На початковій стадії роботи ця

лабораторія використовує набір стандартних експериментальних методів, які широко використовуються в сучасних дослідженнях, але, технології штучного інтелекту, впроваджені в керуючий комп'ютер лабораторії, дозволяють їй вчитися і діяти, використовуючи творчий підхід. А це, в свою чергу, є демонстрацією того, як найсучасніші Інформаційні технології зможуть перетворити область наукових досліджень в самих різних областях.

Нещодавно представники компанії IBM оголосили про завершення розробки і створення повністю автоматичної роботизованої хімічної лабораторії RoboRXN, управління якою здійснює "хмарна" система штучного інтелекту. Мета створення цього комплексу полягає в наданні максимально можливої допомоги вченим-хімікам, що займаються пошуками і створенням нових матеріалів. І робитися це буде за допомогою нової лабораторії більш швидким і ефективним шляхом, ніж забезпечує загальноприйнятий емпіричний метод, метод проб і помилок.

Протягом всієї історії люди розробляли нові матеріали шляхом змішування в певних пропорціях інших матеріалів, і використовуючи, іноді, каталізатори для прискорення хімічних реакцій. А основний метод, що використовувався при цьому, метод проб і помилок, є довгим і досить дорогим заняттям і на сьогоднішній день. Згідно зі статистикою, на розробку нового корисного матеріалу витрачається в середньому до 10 мільйонів доларів і цей процес займає від п'яти до десяти років.

За допомогою впровадження лабораторії RoboRXN компанія IBM планує кардинально змінити наявну ситуацію в області розробок нових матеріалів. В основі цієї лабораторії лежать принципи розробленої в 2018 році системи IBM RXN for Chemistry, якій треба було тільки вказати цільову молекулу, а система видавала список компонентів і покрокову інструкцію для синтезу цієї молекули. Нова ж лабораторія RoboRXN зможе самостійно провести експериментальну перевірку отриманих інструкцій, відкидаючи в сторону непрацюючі варіанти.

Одним із прикладів застосування лабораторії RoboRXN може бути синтез аналогів речовин натурального походження. Уявіть собі, що в лісах Амазонки, наприклад, знайдено рослину, застосування якого уповільнює розвиток хвороби Альцгеймера. Більш ретельні дослідження дозволяють виділити активний інгредієнт, яким є органічна молекула певного типу. І наступним кроком стане розробка технології, що дозволяє синтезувати штучний варіант цієї ж молекули, на що зазвичай йдуть роки досліджень, в ході яких будуть витрачені шалені суми грошей.

За допомогою лабораторії RoboRXN цей процес стане більш швидким. Через деякий час після завантаження даних про цільову молекулу, вчені отримають перевірену

експериментально інструкцію по їх синтезу. Однак, даний спосіб проведення подібних досліджень не бере до уваги деяких очевидних речей, система не може гарантувати, наприклад, що розроблений нею процес синтезу буде економічно рентабельним. Крім того, зараз в системі лабораторії RoboRXN існує ще одне обмеження на кількість етапів синтезу, яке дорівнює 5. Але в майбутньому, у міру накопичення масиву експериментальних даних, кількість етапів може бути збільшено, в теорії, до нескінченності.

Література:

1. *https://www.dailytechinfo.org/infotech/9836-sozdana-sistema-iskusstvennogo-intellekta-rasschityvayuschaya-rezultaty-organicheskih-himicheskih-reakciy.html*
2. *https://www.dailytechinfo.org/infotech/9968-iskusstvennyy-intellekt-uspeshno-spravilsya-s-razrabotkoy-i-planirovaniem-kvantovyh-eksperimentov.html*
3. *https://www.dailytechinfo.org/infotech/10953-roborxn-polnostyu-robotizirovannaya-himicheskaya-laboratoriya-pod-upravleniem-iskusstvennogo-intellekta.html*

ПРИСТРІЙ, ЗДАТНИЙ БАЧИТИ КРІЗЬ ХМАРИ І ТУМАН

Костроміна Марія Олександрівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Погана погода робить процес водіння автомобіля надзвичайно небезпечною справою незалежно від того, хто керує цим автомобілем, людина або автоматична система. Пристрій, здатний бачити крізь хмари і туман, використовує світло лазера, який генерує короткочасні спалахи. Відбитий туманом або перешкодою світло реєструється спеціальним датчиком і комп'ютер обчислює час, що вимагається датчику для того, щоб знову прийти в норму після лазерного імпульсу.

Однією з великих проблем для систем управління автономними автомобілями-роботами є густий туман, який перешкоджає роботі численних камер і датчиків. І вчені зі Стенфордського університету, взявши за основу широко застосовувану технологію лазерного сканування LIDAR, доповнили її рядом високоефективних програмних алгоритмів і отримали систему, здатну бачити об'єкти, приховані за пеленою густого туману.

Розроблена вченими система здатна відновити тривимірні зображення прихованих об'єктів за допомогою аналізу руху частинок світла - фотонів. Для цього в складі системи є лазер, постійно скануючий простір. Частина фотонів лазерного променя розсіюється туманом, але інший, меншою, частини все ж вдається дістатися об'єкта і відбитися від його поверхні.

Частина відбитих фотонів також розсіюється туманом і лише ліченим одиницям з них вдається дістатися до

надвисокочутливого датчика, здатного реєструвати час прибуття та інші параметри одиничних фотонів. Використовуючи ці крупиці вихідної інформації, складні програмні алгоритми виконують процедури фільтрації, апроксимації та інші, які дозволяють відтворити тривимірне зображення об'єкта, прихованого за пеленою туману.

Під час випробувань Стенфордська система успішно відновила зображення об'єкта, поміщеного за листом піни товщиною в 1 дюйм (2.54 сантиметри), яка імітувала більш товстий шар вельми густого туману. Якості отриманого тривимірного зображення було достатньо для визначення форми об'єкта і відстані до нього. Іншими словами, система керування автомобілем-роботом отримала б в таких умовах всю інформацію, необхідну для того, щоб уникнути аварійної ситуації.

Система, створена Стенфордськими вченими, є далеко не першою подібною лазерною системою. Однак, за рахунок деяких тонкощів, вченим вдалося обійти ряд обмежень, які перешкоджають роботі інших систем, деякі з яких здатні за один прохід сканувати туман тільки на певну глибину, наприклад.

І у висновку слід зазначити, що дана система може бути використана не тільки в технологіях управління рухом автомобілів-роботів і безпілотних літальних апаратів. Ще однією потенційною областю застосування системи "протитуманного комп'ютерного бачення" є дослідження Землі та інших планет з супутників, що рухаються по низькій орбіті. В такому випадку система може забезпечити сканування поверхні планети крізь хмарний шар або каламутну атмосферу, наповнену частинками пилу, наприклад.

Література:

1. https://www.dailytechinfo.org/auto/10113-novaya-lazernaya-sistema-pozvolit-avtomobilyam-robotam-videt-skvoz-gustoy-tuman.html

2. https://www.dailytechinfo.org/auto/9896-1000-kratnoe-uvelichenie-razreshayuschey-sposobnosti-datchikov-pozvolit-avtomobilyam-robotam-videt-skvoz-tuman.html

3. https://www.dailytechinfo.org/auto/10960-stenfordskie-uchenye-sozdali-ustroystvo-sposobnoe-videt-skvoz-oblaka-i-tuman.html

БЕЗПЕКА ФІНАНСОВОГО СЕКТОРА

Кузьменко Олександр Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

В контексті кібербезпеки 2019 рік пройшов під знаком APT-атак, пошуку апаратних вразливостей і гучних витоків. За той час, поки керівники компаній приходили до усвідомлення необхідності вибудовувати дійсно ефективну систему інформаційної безпеки, злочинці міцно влаштувалися в кіберпросторі. Найбільш яскравим прикладом став ринок в Дарквеб, де продається маса заборонених товарів і послуг, в тому числі хакерські утиліти і доступ до вже зламаним інфраструктур. Крім того, злочинці продовжують використовувати неграмотність користувачів в питаннях забезпечення власної безпеки.

Ключові слова: інтернет-банкінг, фішинг, платіжні системи, кібербезпека, шкідливе пз.

За перші три квартали 2019 роки було зафіксовано 61 атаку на фінансові компанії (за аналогічний період 2018 року їх були 69, а за весь 2018 рік - 92). Причому в 74% атак використовувався фішинг і в 80% атак - шкідливе ПЗ.

Припускаємо, що незначний спад числа кібератак на фінансові організації пов'язаний з декількома факторами. По-перше, помітне значне зниження частки масових атак на такі установи - наприклад, в третьому кварталі 2019 року всього 4% зафіксованих атак носили масовий характер, а в аналогічний період роком раніше цей показник був на рівні 32%. Це можна пояснити тим, що більшість банків, особливо великих, сьогодні готові ефективно відбити масову атаку (наприклад розсилку шифрувальника), і хакери сконцентрували свою увагу на інших, менш захищених галузях.

По-друге, число цілеспрямованих атак на фінансові організації не знижується, угруповання не тільки оновлюють свою інфраструктуру, а й звертають увагу на нові регіони, вибирають жертв, менш готових до таких атак.

У першому і в другому кварталах виділялись атаки APT-угруповань Cobalt і Silence, а також ще однієї групи, яка використовувала мережеву інфраструктуру, схожу з інфраструктурою групи FinTeam. У третьому кварталі найбільш активною стала група Cobalt в Росії, Казахстані та країнах Європи, а також фішингові розсилки групи TA505 на адресу європейських і африканських банків і групи RTM на адресу банків Росії і Білорусії.

Штучний інтелект все частіше застосовується в фінансових організаціях. Дослідження банківського ринку свідчать про розширення сфери застосування цієї технології, перш за все машинного навчання. Машинне навчання не тільки забезпечує зручність кінцевого споживача при використанні банківських сервісів, а й успішно застосовується для протидії шахрайству в банківській сфері.

Банкомати та платіжні термінали

За даними некомерційної організації Європейська асоціація безпечних операцій (EAST), у першій половині 2019 року основний збиток від кібератак на системи самообслуговування європейських банків припав на атаки проти платіжних терміналів (124 мільйони євро) - при тому, що в результаті атак на банкомати з використанням ВПО і техніки black box 7 був зафіксований лише незначний фінансовий збиток, що не перевищує 1000 євро.

Зростає кількість шахрайських операцій з безконтактними платежами; Це пов'язано, головним чином, з операціями нижче обмежень CVM (Метод перевірки власника картки), в яких користувачеві не потрібно вводити PIN-код для підтвердження транзакцій.

Якщо 15 років тому кількість постачальників фінансових послуг була обмежена банком - емітентом карток, компанією, що надає послуги еквайрингу, та платіжною системою (Visa, MasterCard), то зараз набагато більше людей мають доступ до карток та пов'язаної з ними інформації: Apple Pay і Samsung Pay, виробники терміналів mPOS, оператори мобільних мереж, виробники смартфонів тощо. Кількість "свідків платежів" збільшується, усі вони мають непрямий доступ до банківського рахунку та інформації власника картки, а отже, ризик збільшується витік та шахрайські операції. Подібна ситуація склалася з інтернет-банкінгом.

Цього року в Європейському Союзі вони почали впроваджувати нову директиву про платіжні операції PSD2, яка покликана створити умови для інновацій у фінансовому секторі та забезпечити додатковий захист клієнтів.

Директива передбачає:

- надання банкам відкритого API для всіх сторонніх постачальників фінансових послуг (Open Banking);
- вимога посилити аутентифікацію платника (сильна автентифікація клієнта). Ця вимога вказує на обов'язкову двофакторну автентифікацію, наприклад, на необхідність періодично перевіряти наявність двох з трьох елементів (PIN-код, відбиток пальця, обличчя тощо). Відповідно до цієї вимоги, наприклад, після кожних п'яти безконтактних операцій платник буде зобов'язаний вставляти картку в зчитувач мікросхем, а мобільний додаток періодично запитуватиме PIN-код, навіть якщо буде введена функція авторизації відбитків пальців.

Рис.1. Схема взаємодії учасників дерективи

Комплексне впровадження таких заходів покращить безпеку банківських систем, особливо в такій чутливій галузі, як безконтактні платежі та оплата карткою.

Це, безсумнівно, великий крок до безпеки фінансового сектору і на державному рівні, і ми можемо лише вітати появу подібних стандартів у сфері платежів у всьому світі, в тому числі і в нашій країні.

Література:

1. Досвід впровадження PSD2 / Open Banking в Європейському союзі URL: http://futurebanking.ru/post/3788

2. ATM malware and logical attacks fall in Europe URL: https://www.association-secure-transactions.eu/files/ATM-malware-and-logical-attacks-fall-in-Europe-for-release-to-the-media-on-9th-October-2019.pdf

СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА СТАНДАРТИЗАЦІЇ. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

Кузьменко Олександр Дмитрович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Найважливішим аспектом розвитку сучасних телекомунікаційних систем є їх стандартизація. Стандартизація необхідна всім мешканцям світу телекомунікацій, включаючи виробників електронних компонентів, виготовлювачів апаратури, розробників мереж і кінцевих користувачів. Перш за все стандартизація означає масовість виробництва, що веде до низьких цін і широкому розповсюдженню технологій.

Ключові слова: IEEE, стандартизація, обчислювальна техніка, товариство, COVID-19.

В переліку стандартизуючих організацій дуже важливе місце займає Інститут інженерів з електротехніки та електроніки - IEEE (Institute of Electrical and Electronics Engineers). Досить сказати, що членами IEEE є ANSI і ISO. IEEE випускає свої власні стандарти, які мають загальносвітове значення. Як правило, вони потім затверджуються ISO та / або ITU.

Інститут інженерів електротехніки та електроніки, Inc. (IEEE) - це найбільша у світі технічна професійна асоціація, яка налічує понад 350 000 членів у 150 країнах. Це некомерційна організація, яка займається розвитком теорії та застосування електротехніки та електроніки та інформатики. Завдяки своїм членам IEEE є провідним авторитетом у сферах, починаючи від аерокосмічної галузі, комп'ютерів та телекомунікацій до біомедицини, електроенергетики та побутової електроніки.

IEEE служить інженерам-електрикам та вченим з 1884 року, коли група винахідників та підприємців, включаючи Томаса Едісона та Олександра Грема Белла, заснувала Американський інститут інженерів-електриків (AIEE). У 1912 р. Фахівці з радіотехніки створили окреме міжнародне товариство - Інститут інженерів-радіотехніків (IRE). У 1963 р. AIEE та IRE об'єдналися, щоб сформувати IEEE.

Сьогодні IEEE виробляє майже 30 відсотків світової літератури в галузі електротехніки, електроніки та обчислювальної техніки, а щороку спонсорує або спонсорує понад 300 технічних конференцій. Вона також виробила 900 активних галузевих стандартів, більше третини з яких впливає на інформаційні технології та комп’ютерну галузь.

IEEE складається з 300 місцевих секцій та 1200 студентських розділів, а також 40 товариств та рад, які охоплюють широкий спектр областей технічного інтересу. Найбільшим із товариств інституту є Комп’ютерне товариство IEEE.

Комп'ютерне товариство IEEE

Простежуючи своє походження з 1946 року, Комп’ютерне товариство є провідним постачальником технічної інформації та послуг для світових обчислювальних фахівців. Місія товариства полягає в просуванні комп'ютерної та інформаційної обробки інформації та техніки; сприяти професійній взаємодії; та інформуйте учасників про останні події.

Функції товариства:

Суспільство є лідером у розробці стандартів для обчислювальної галузі, підтримуючи понад 200 груп з розробки стандартів у дванадцяти основних технічних областях. Серед цих стандартів - бездротові мережі, проектування веб-сторінок

та програмне забезпечення. Стандарти IEEE широко прийняті промисловістю для забезпечення стабільної працездатності та функціональності. Одним із прикладів є стандарт перевірки та перевірки програмного забезпечення IEEE 1012, який, серед іншого, допомагає забезпечити безпеку літаків та атомних електростанцій та забезпечити стабільну роботу стільникових телефонів, звукових сигналів та відеоігор.

Товариство спонсорує програму студентських нагород та стипендій. Міжнародний конкурс дизайнерів IEEE Computer Society (CSIDC) - це конкурс з проектування інформатики та інженерних систем, відкритий для команд студентів з усього світу. Стипендія Річарда Е. Мервіна присуджує до чотирьох щорічних стипендій для зразкових добровольців студентів або студентів комп'ютерного товариства. Стипендія видатного студента Ланса Стаффорда Ларсона отримує студент, який подає найкращі студентські роботи з комп'ютерної тематики. Премія Upsilon Pi Epsilon / Computer Society була створена для заохочення академічної досконалості та пропонує щороку до чотирьох нагород. Upsilon Pi Epsilon - Міжнародне почесне товариство обчислювальних наук.

Стандарти IEEE щодо реагування на глобальну надзвичайну ситуацію в галузі громадського здоров'я COVID-19

IEEE усвідомлює, що багато хто прямо чи опосередковано бере участь у боротьбі з COVID-19 та його наслідками для глобальної охорони праці, досліджень, інфраструктури, зв'язку тощо. IEEE визначила статті та стандарти з цифрової бібліотеки IEEE Xplore, які можуть допомогти дослідникам зрозуміти та керувати різними аспектами пандемії COVID-19 та технологіями, які можна використовувати для боротьби з нею.

IEEE безкоштовно зробила ці стандарти доступними, щоб допомогти пришвидшити реакцію розвитку на поточну світову кризу охорони здоров'я. Тепер ці стандарти є вільними для доступу, з додатковими правами для всіх типів повторного використання, включаючи аналіз повного тексту та даних.

Література:

1. Веб-сайт Комп'ютерного товариства IEEE URL: http://www.computer.org

2. Веб-сайт Institute of Electrical and Electronics Engineers, Inc. URL: http://www.ieee.org/

3. Інформаційний бюлетень студентів комп'ютерного товариства IEEE URL: http://www.computer.org/students/looking/

КОНФІГУРУВАННЯ ПАРАМЕТРІВ БЕЗПЕКИ ОС

Кукшин Дарія Вікторівна

Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Налаштування безпеки Windows можуть допомогти захистити контролери домену, сервери, клієнти та інші ресурси вашої організації. Без налаштувань безпеки Windows ви не зможете перевірити автентифікацію користувачів, обмежити доступ до ресурсів, керувати членством у групі чи реєструвати журнали змін. Microsoft розробила налаштування безпеки Windows для боротьби з динамічним характером уразливостей. Саме архітектура Windows як послуга надає Майкрософт можливість постійно впроваджувати технології безпеки, щоб гарантувати, що Windows 10 залишається їх найбільш безпечною на сьогоднішній день операційною системою. Нижче наведено декілька найпопулярніших налаштувань безпеки Windows, розроблених для забезпечення безпеки.

Налаштування параметра за допомогою консолі локальної політики безпеки

1. Щоб відкрити локальну політику безпеки, на початковому екрані введіть secpol.msci натисніть клавішу Enter.
2. У розділі Параметри безпеки в дереві консолі виконайте одну з таких дій.

- Натисніть політики облікових записів, щоб змінити політику паролів або політику блокування облікових записів.
- Натисніть «Локальні політики», щоб змінити політику аудиту, Призначення прав користувача і Параметри безпеки.

3. Коли ви знайдете параметр політики в області відомостей, двічі натисніть на політику безпеки, яку ви хочете змінити.
4. Змініть параметр політики безпеки, а потім натисніть кнопку ОК.

Налаштування параметра політики безпеки за допомогою консолі редактора локальної групової політики

Для виконання цих процедур необхідно мати відповідні дозволи на встановлення і використання консолі управління (MMC), а також для оновлення об'єкта групової політики (GPO) на контролері домену [1].

1. Відкрийте редактор локальних групових політик (gpedit.msc).
2. У дереві консолі натисніть «Конфігурація комп'ютера», виберіть пункт Параметри Windows, а потім - Параметри безпеки.
3. Виконайте одну з таких дій.

- Натисніть політики облікових записів, щоб змінити політику паролів або політику блокування облікових записів.
- Натисніть «Локальні політики», щоб змінити політику аудиту, Призначення прав користувачів та Параметри безпеки.

4. В області відомостей двічі натисніть параметр політики безпеки, який ви хочете змінити.

5. Змініть параметр політики безпеки, а потім натисніть кнопку ОК.

Налаштування параметра для контролера домену

Нижче описано, як налаштувати параметр політики безпеки тільки для контролера домену (з контролера домену).

1. Щоб відкрити політику безпеки контролера домену, в дереві консолі знайдіть політику GroupPolicyObject \ [ім'я комп'ютера], натисніть кнопку «Конфігурація комп'ютера», виберіть пункт Параметри Windows, а потім - Параметри безпеки.

2. Виконайте одну з таких дій.

- Двічі натисніть на політики облікових записів, щоб змінити політику паролів, політику блокування облікових записів чи політику Kerberos.
- Натисніть «Локальні політики», щоб змінити політику аудиту, Призначення прав користувача або Параметри безпеки.

3. В області відомостей двічі натисніть на політику безпеки, яку ви хочете змінити.

4. Змініть параметр політики безпеки, а потім натисніть кнопку ОК.

Аудит системних подій

Визначає, чи слід виконувати аудит, коли користувач перезавантажується або завершує роботу комп'ютера, або коли виникає подія, яка впливає на безпеку системи або журнал безпеки.

Якщо ви визначаєте цей параметр політики, ви можете вказати, чи слід проводити аудит успіхів, аудит відмов або взагалі не проводити аудит для типу події. Аудит успіхів призводить до створення запису аудиту при успішному спробі входу. Аудит відмов призводить до створення запису аудиту при невдалій спробі входу.

Щоб відключити аудит, в діалоговому вікні властивості для цього параметра політики встановіть прапорець визначити наступні параметри політики і зніміть прапорці успіх і відмова.

За замовчуванням:

- Успіх на контролерах домену.
- Без аудиту на рядових серверах.

Управління журналом аудиту та безпеки

Цей параметр політики визначає, які користувачі можуть задавати параметри аудиту доступу до об'єктів для окремих ресурсів, таких як файли, об'єкти Active Directory і розділи реєстру[2]. Ці об'єкти визначають системні списки керування

доступом (SACL). Користувач, якому призначено це право користувача, може також переглядати і очищати журнал безпеки в засобі перегляду подій.

Можливі значення:

- Визначається користувачів список облікових записів
- Адміністратори
- НЕ визначено

Рекомендації:

- Перш ніж видаляти це право з групи, перевірте, чи залежить додаток від цього права.
- Як правило, призначення цього права для груп, Крім адміністраторів, не є обов'язковим.

Location: Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignment

Значення за замовчуванням: за замовчуванням цей параметр є адміністратором на контролерах домену і на окремих серверах.

У наведеній нижче таблиці перераховані фактичні і діючі значення політики за замовчуванням для найостанніших підтримуваних версій Windows. Значення за замовчуванням також можна знайти на сторінці властивостей політики [3].

Тип сервера або об'єкт групової політики	**Значення за замовчуванням**
Default Domain Policy	Не визначено
Політика контролера домену за замовчуванням	Адміністратори
Параметри за замовчуванням для автономного сервера	Адміністратори
Діючі параметри за замовчуванням для контролера домену	Адміністратори
Діючі параметри за замовчуванням для рядового сервера	Адміністратори
Діючі параметри за	Адміністратори

замовчуванням для клієнтського комп'ютера	

Табл. 1 Значення політик за замовчуванням

Управління політикою

У цьому розділі описані компоненти, засоби і рекомендації, які допоможуть в управлінні цією політикою.

Для активації цього параметра політики не потрібне перезавантаження комп'ютера. Зміни прав користувача вступають в силу при його наступному вході в обліковий запис.

Аудит для доступу до об'єктів не виконується до тих пір, поки ви не включите їх за допомогою редактора локальних групових політик, консолі управління груповими політиками (GPMC) або засоби командного рядка Auditpol.

Групова політика

Параметри застосовуються в зазначеному нижче порядку за допомогою об'єкта групової політики (GPO), який буде перезаписувати параметри на локальному комп'ютері при наступному оновленні групової політики[3]:

1. Параметри локальної політики
2. Параметри політики сайту
3. Параметри політики домену
4. Параметри політики підрозділи

Якщо локальне налаштування недоступне, це вказує на те, що об'єкт GPO, який в даний час управляє цим параметром

Питання безпеки:

1. Уразливість

Будь-який користувач, який має право управління аудитом і журналом безпеки, може очистити журнал безпеки, щоб стерти важливі докази про несанкціонований дії.

2. Протидія

Переконайтеся в тому, що тільки локальна група адміністраторів має право користувача Управління аудитом і журналом безпеки.

3. Можливий вплив

Налаштування за замовчуванням для обмеження прав користувача на Управління аудитом і журналом безпеки для локальної групи адміністраторів.

Аудит файлової системи

Аудит файлової системи визначає, чи буде операційна система створювати події аудиту при спробі користувачів отримати доступ до об'єктів файлової системи.

Події аудиту генеруються тільки для об'єктів з налаштованими системними списками управління доступом

(SACL) і тільки в тому випадку, якщо запитаний тип доступу (наприклад, "запис", "читання" або "зміна") і обліковий запис, в результаті якої запит відповідає параметрам в списку SACL[1].

Якщо включений аудит успіхів, запис аудиту створюється кожен раз, коли будь-яка обліковий запис успішно отримає доступ до об'єкта файлової системи, що має відповідний список SACL. Якщо включений аудит відмов, при кожній спробі користувача отримати доступ до об'єкта файлової системи, що має відповідний список SACL, створюється запис аудиту.

Ці події важливі для відстеження активності для об'єктів файлів, які є важливими або важливими і вимагають додаткового контролю.

Гучність події: залежить від настройки SACL для файлової системи.

Для списку SACL файлової системи, що використовується за умовчанням, не генерується жодних подій аудиту.

Ця категорія дозволяє проводити аудит спроб доступу користувачів до об'єктів файлової системи, видалення об'єктів файлової системи, змін дозволів і дій, пов'язаних зі створенням і жорстким зв'язком.

Рекомендується розробити політику спостереження за безпекою файлової системи і задати відповідні елементи управління доступом для об'єктів файлової системи для різних шаблонів і ролей операційної системи. Не вмикайте цю підкатегорію, якщо ви не плануєте використовувати і аналізувати зібрані відомості. Важливо також видалити неефективні елементи списку SACL.

Література:

1. Windows security baselines [Електронний ресурс] – Режим доступу: World Wide Web. – URL: ***https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines***

2. Аудит системных событий [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/basic-audit-system-events

3. Управление журналом аудита и безопасности [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log

СВІТ ТЕЛЕКОМУНІКАЦІЙ ТА СТАНДАРТИЗАЦІЇ

Кучеренко Кирило Максимович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Стандартизація в галузі телекомунікацій. У вузькому значенні слова «стандарт» -це «нормативний документ по стандартизації, розроблений, як

правило, на основі згоди, що характеризується відсутністю заперечень по суттєвих питаннях у більшості заінтересованих сторін, прийнятий (затверджений) визнаним органом (підприємством)».

Ключові слова: стандартизація, ITU, ISO, МОС, телекомунікації.

Стандарти пов’язують нас із надійними способами спілкування, кодексами практики та рамками для співпраці. Різноманітні спільноти, багаті унікальними навичками та засобами виробництва, знаходять взаємну вигоду в торгівлі та на більшому ринку, який вона створює, але цього можна досягти лише шляхом застосування загальних стандартів. Міжнародні стандарти говорять про різноманітність нашого взаємопов’язаного світу, вводячи однаковість інтерфейсів, де ми повинні бути впевнені, що всі ми на однакових умовах.

Стандарти формують довіру. Вони відіграють участь майже в кожному споживаному нами продукті та в кожному процесі, який готує їх до споживання. Продукти чи послуги, що відповідають міжнародним стандартам, просочені надійними символами якості, безпеки та сумісності. Інформаційно-комунікаційні технології (ІСТ), такі як мобільні телефони, планшети та персональні комп’ютери, мають широкий спектр функцій, але всі з’єднуються та функціонують загальною мовою, передбаченою міжнародними стандартами. Промисловість ІСТ покладається на технічну стандартизацію в тій мірі, у якій конкурує лише кілька інших галузей промисловості. Технічна стандартизація встановлює технічні норми для складних систем і має вирішальне значення у захопленні та стимулюванні інновацій, забезпечуючи життєву силу мереж ІСТ. Такі мережі потребують загальних стандартів, щоб забезпечити взаємозв'язок та сумісність.

Такі органи, як Міжнародний союз електрозв'язку (ITU), є основним засобом забезпечення співпраці та співпраці, необхідних для встановлення міжнародних стандартів. Правила та процедури ITU сприяють відкритості та прозорості, забезпечуючи середовище, де новатори з конкуруючих компаній можуть об'єднуватися для розробки міжнародних стандартів, що відповідають їх потребам у загальних платформах для зростання ІСТ та інновацій.

Всесвітня асамблея стандартизації телекомунікацій проводиться кожні чотири роки і визначає наступний період навчання для ITU-T. Асамблея розглядає методи роботи, включаючи процеси затвердження, робочі програми та структуру навчальної групи. Матеріали містять резолюції та думки, прийняті Асамблеєю, рекомендації щодо організації роботи ITU-T та обидві рекомендації, затверджені з

попереднього періоду дослідження, а також питання, затверджені на наступний період дослідження.

Кінцевою метою стандартизації ITU є встановлення високоякісних міжнародних стандартів, розроблених із використанням відкритого, всеохоплюючого процесу, що відповідає потребам новаторів ІСТ у найрізноманітніших галузях промисловості. Процес стандартизації ITU, зумовлений внеском, відповідає давньому прагненню до прийняття рішень на основі консенсусу. Принципи, що лежать в основі процесу, забезпечують, щоб усі голоси були почуті, що стандартизаційні зусилля не сприяли певним комерційним інтересам, і щоб отримані стандарти мали консенсусну підтримку різноманітного кола зацікавлених сторін, що становлять членство в ITU. Інклюзивність платформи стандартизації підтримується програмою ITU Bridging the Standardization Gap, яка допомагає країнам, що розвиваються, покращити свою здатність брати участь у розробці та впровадженні міжнародних стандартів ІСТ. Захищаючи принципи, що керують стандартизацією ITU, та вітаючи нові громади як члени ITU підтримує появу надійного ІСТ-середовища, здатного підтримувати соціальний та економічний розвиток у всіх регіонах світу.

Література:

1. Сектор стандартизації телекомунікацій ITU. URL: https://www.itu.int/en/ITU-T/Pages/default.aspx

2. *Національна комісія державного регулювання комунікацій і інформатизації. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=1&language=en*

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ ВНУТРІШНЬОЇ ЗАГРОЗИ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ МЕХАНІЗМУ ВИЯВЛЕННЯ АНОМАЛІЙ В SIEM-СИСТЕМАХ

Ліщук Інна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Опитування інсайдерських досліджень показують, що конкретна поведінка людей, а не їх демографічні чи психологічні особливості, часто є найкращими показниками ризику, що може перетворитися на інсайдерську загрозу. Програмне забезпечення (ПЗ) для моніторингу мережі є критичним інструментом для виявлення внутрішніх та зовнішніх кіберзагроз. Після впровадження ПЗ для моніторингу, відповідні фахівці повинні стежити за мережею, тобто за аномальною діяльністю користувачів. Для цього і існує механізм виявлення аномалій.

Правила виявлення аномалій перевіряють результати збереженого потоку або виробляють пошук подій, щоб виявити, коли в мережі виникають незвичайні шаблони трафіку. Правила виявлення аномалій вимагають, щоб був збережений пошук, згрупований на основі загального параметра. Цьому пошуку, як правило, потрібно накопичити дані, перш ніж правило аномалій поверне будь-які результати для виявлення шаблонів аномалій, порогів або змін поведінки.

Механізм виявлення аномалій (ADE) складається з: правил аномалій, правил порогів та правил поведінки [1].

Правила аномалій – перевірка трафіку подій і потоків на наявність змін в короткострокових подіях, коли проводиться порівняння протягом більш тривалого періоду часу. Наприклад, нові служби або програми, що з'являються в мережі, аварійне завершення роботи веб-сервера, брандмауери, які починають масово відмовляти в трафіку.

Рис. 1 показує перевірку, чи середнє значення протягом поточного короткого інтервалу часу відхиляється вище заданого відсотка від базової лінії протягом більш тривалого періоду часу.

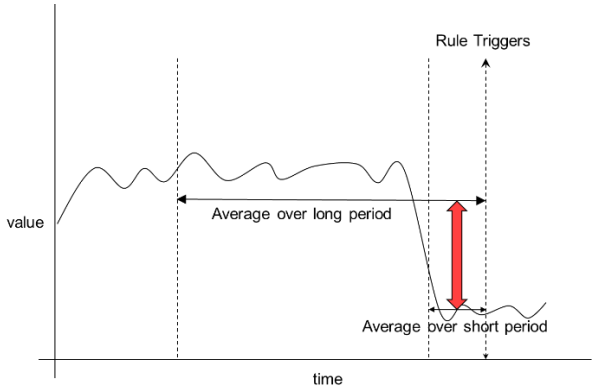


Рис. 1. Спрацювання правила аномалії

Правила порогів – це події або потоки, що перевіряються на наявність операції, яка більше або менше заданого діапазону. Ці правила корисні для виявлення: змін використання смуги пропускання в додатках, служб, які невдало завершили роботу, користувачів, які використовують VPN, вихідного трафіку великого обсягу тощо.

Рис. 2 показує перевірку значень властивостей на предмет перевищення значень встановленої верхньої або нижньої межі.

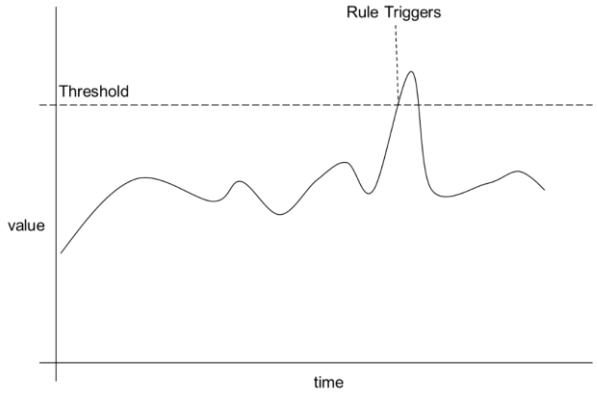


Рис. 2. Спрацювання правила порогу

Правила поведінки – це перевірка зміни значень в звичайних шаблонах для подій або потоків, щоб виявити аномалії. Наприклад, у поштового сервера є відкрита ретрансляція і він раптово взаємодіє з багатьма хостами. Системи IPS запускаються, щоб згенерувати численні операції сповіщень.

Рис. 3 зображує перевірку, чи поточні значення властивостей відхиляються від сезонних шаблонів. Правило поведінки вивчає швидкість або обсяг значення властивості протягом встановленого часу для заданої базової лінії.

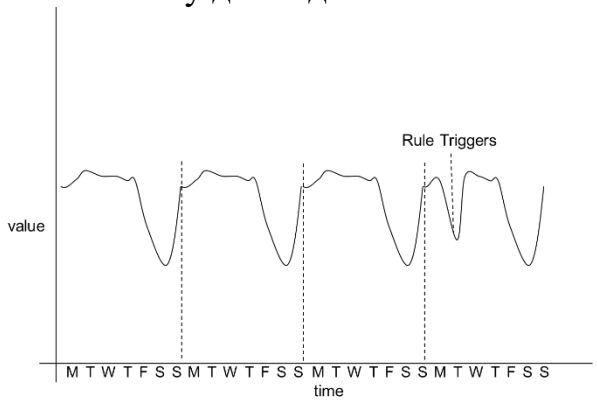


Рис. 3. Спрацювання правила поведінки

Отже, задля того, щоб вберегти організацію та й інформаційну корпоративну мережу в цілому, потрібно вчасно виявляти внутрішні загрози. Тому варто зосередити увагу на превентивних заходах та програмних засобах, комплексних рішеннях для моніторингу та реєстрації інсайдерської активності користувачів, що позначають підозрілу поведінку користувачів та надають інформацію, необхідну для реагування на інциденти порушення безпеки.

Література:

1. Anomaly detection rules [Електронний ресурс] // IBM Knowledge Center – Режим доступу до ресурсу: https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_rul_anomaly_detection.html.

АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ВНУТРІШНЬОЇ ЗАГРОЗИ ПРОЦЕСАМ ФУНКЦІОНУВАННЯ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ USER (AND ENTITY) BEHAVIORAL ANALYTICS

Ліщук Інна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Забезпечення IT-безпеки підприємства вимагає комплексного підходу, який збалансовує захист як від зовнішніх, так і від внутрішніх загроз. Тим часом представники бізнесу приділяють достатньо уваги лише зовнішнім загрозам (шкідливим кодам, мережевим атакам і спаму), в той час як дії самих співробітників компанії здебільшого не контролюються. В даний час тенденції в сфері безпеки зводяться до того, що увага зосереджується на людині та її поведінці, так як все ж таки саме людина є основним джерелом ризиків, загроз, порушень та інцидентів. Основним інструментом для аналізу поведінки користувача є система User Behavior Analytics.

User (and Entity) Behavioral Analytics (UEBA / UBA) – клас систем, що дозволяють на основі масивів даних про користувачів за допомогою алгоритмів машинного навчання і статистичного аналізу будувати моделі поведінки користувачів і визначати відхилення від цих моделей, як в режимі реального часу, так і ретроспективно. Як джерела даних для UEBA-систем можуть виступати файли журналів серверних і мережевих компонентів, журнали систем безпеки, локальні журнали з кінцевих станцій, дані з систем автентифікації і навіть зміст листування в соціальних мережах, месенджерах і поштових повідомленнях [1].

Нижче наведено короткий опис найбільш популярних продуктів в сегменті UBA/UEBA для виявлення внутрішньої загрози в корпоративній інформаційній системі.

1. Exabeam Advanced Analytics - на думку експертів Gartner, продукт Exabeam Advanced Analytics є одним з кращих в категорії UBA. В основі Exabeam Advanced Analytics лежить власна технологія, названа «Statefull User Tracking», яка в повністю автоматичному режимі будує нормальний профіль користувачів, спираючись на інформацію про сесії, пристрої, IP-адреси і облікові записи користувачів. Платформа Exabeam ліцензується за кількістю користувачів і не прив'язується до обсягу оброблюваних даних, як класичні SIEM-системи.

2. Microsoft Advanced Threat Analytics (ATA Microsoft) - допомагає запобігати збиткам від кібератак і в реальному часі показує найважливішу інформацію про кожну атаку на часовій шкалі. Microsoft ATA може забирати дані як класичними засобами Microsoft (зі збирача подій Windows), так і з сторонніх

SIEM-систем. Microsoft ATA виявляє три типи загроз: атака зловмисників, аномальна поведінка і проблеми або ризики безпеки.

3. Splunk User Behaviour Analysis - виявляє невідомі загрози і аномальну поведінку за допомогою машинного навчання, автоматизує об'єднання сотень аномалій в єдину загрозу, що значно спрощує обов'язки аналітика безпеки, використовує глибокі слідчі можливості і потужні базові характеристики поведінки для будь-якої сутності, аномалії або загрози;

4. Forcepoint UEBA - дозволяє командам безпеки проактивно відстежувати всередині організації аномальну поведінку з високим рівнем ризику, такі як: скомпрометовані облікові записи, корпоративне шпигунство, крадіжка інтелектуальної власності та шахрайство.

5. ObserveIT Insider Threat Management - відмінною рисою архітектури рішення ObserveIT є наявність клієнтських агентів, що дозволяють здійснювати проактивне блокування певних дій користувача, в тому числі при визначенні поведінкових аномалій в них. ObserveIT, на відміну від класичних UEBA-рішень, ліцензується за кількістю кінцевих станцій, що знаходяться під управлінням системи.

6. IBM QRadar UBA - розширення для SIEM-системи IBM QRadar., що фокусується виключно на поведінковому аналізі користувачів. Виставлення оцінок ризику кожному користувачеві проводиться, як на основі простих статистичних правил, так і за допомогою методів машинного навчання [2].

Хоча рішення UEBA з'явилися не так давно, вони швидко стали популярними у великих корпораціях. В ядро будь UEBA-системи включаються технології по роботі з великими масивами даних, тому, багато постачальників включають функціональність UEBA в інші інструменти безпеки, такі як SIEM, системи аналізу мережевого трафіку, управління ідентифікацією та доступом (IAM) тощо.

Отже, внутрішні фахівці найчастіше є слабкою ланкою в системі управління інформаційною безпекою. Демаскувати ці загрози досить важко, тому важливо розуміти, що одним з основних факторів виявлення інсайдерських загроз є моніторинг поведінки користувачів. Вище були наведені найуспішніші програмні продукти, що займаються UBA в інформаційних системах, адже саме інструменти контролю доступу та персоналу, разом з поведінковою аналітикою допоможуть розробити ефективні методи для виявлення внутрішніх загроз та заходи захисту від людського фактору і злочинних намірів.

Література:

1. Матвеев О. Обзор рынка систем поведенческого анализа — User and Entity Behavioral Analytics (UBA/UEBA) [Електронний ресурс] / Олексій Матвіїв. – 2017. – Режим доступу до ресурсу: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba.

2. Advanced Threat Analytics [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/microsoft-365/enterprise-mobility-security/advanced-threat-analytics?rtc=1

ЩО ТАКЕ «ВИТІК ДАНИХ» І ЯК ЗАПОБІГТИ ЦІЙ ЗАГРОЗІ

Лягушкін Іван Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
м. Київ

Як ми можемо спостерігати, за якісь 20 років наш світ кардинально змінився. Система документообігу більшою мірою перейшла в електронний вигляд, і наше життя теж стало більш цифровим. Кожного дня ми користуємося месенжерами, соціальними мережами, браузерами, онлайн банкінгом, здійснюємо онлайн-покупки. І ми задаємося різними питаннями в плані безпеки, на скільки ми в безпеці, на скільки в безпеці наші персональні дані, чи раптом за нами ніхто не слідкує, а може наші дані вже в зацікавлених людей? Давайте з'ясуємо.

Що ж таке витік інформації або витік даних? Витік даних - це коли зацікавлена особа отримує неправомірний доступ до інформації. Зазвичай існує три категорії людей, які можуть стати причиною витоку даних усередині організації.

Випадковий інсайдер

Іноді витік даних може бути випадковою. Наприклад, хтось працював в організації і мав дуже великі привілеї. В цьому випадку папка або файл можуть виявитися в поле зору випадково або внаслідок нездорової цікавості. У випадку зі випадковими інсайдерами розкрита інформація не представляє особливої загрози, але заходи по усуненню проблеми все одно повинні бути зроблені. [1]

Зловмисний інсайдер

Ситуація схожа з попередньою з тією лише відмінністю, що у даного типу інсайдерів нечистоплотні помисли. Зловмисний інсайдер - самий неприємний сценарій серед розглянутих в цій статті, оскільки хтось, до кого була довіра, стає причиною навмисної витоку. Класичний приклад, про який багато хто з вас знають, - Едвард Сноуден. Працюючи в АНБ в якості підрядника, у Сноудена був відповідний рівень доступу, що стало причиною витоку надзвичайно секретної інформації про суперечливі урядових програмах. [1]

Зовнішня загроза

Зовнішня загроза - будь-який зловмисник, який отримує неправомірний доступ до інформації. У цю категорію потрапляє велика група людей з різною мотивацією, починаючи від хакера-початківця і закінчуючи групою хакерів,яка спонсорується урядом. Наслідки від витоків, пов'язаних зі сторонніми діячами, можуть виявитися дуже неприємними. Недавні приклади, що потрапляють в цю категорію, - атаки на компанії Target і Sony. [1]

Що стосується витоку даних, вирішальну роль можуть грати різні чинники. Деякі серед найбільш поширених причин:

- Уразливості в системі.
- Слабкі або повторно використовувані паролі.
- Цільові атаки.
- Надлишкові права доступу.
- Шкідливі програми.
- Фішинг або спуфинг.
- Вкрадені облікові записи.

Хоча витік даних - явище неприємне (деякі навіть скажуть, що неминуче), організація може зробити деякі кроки для мінімізації збитку для даних і систем, а також зберегти репутацію бренду і довіру покупців. Найбільш важливий крок - підготовка. [1]

Існує кілька дієвих способів, які допоможуть знизити ризик витоку та розголошення інформації. Підприємство може використовувати всі методи захисту або тільки кілька з них, адже система безпеки повинна бути економічно вигідною. Збитки від втрати секретної інформації не можуть бути меншими від вартості впровадження і підтримки системи безпеки. Найефективніші способи захисту:

Шифрування

Шифрування – це простий і дієвий метод захисту комерційної таємниці. Сучасні алгоритми шифрування використовують світові стандарти в області криптографії, двосторонній обмін ключами і еліптичні криві для генерації захисту.

Впровадити політику безпеки.

Реалізація політики або програми в сфері безпеки, яка сфокусована не тільки на захист конфіденційної інформації, а й облікових записів, які забезпечують доступ до цієї інформації - критично важливо для зниження ризиків. [2]

Контроль персоналу

Персонал – це найбільш неконтрольоване джерело витоку інформації. Адміністратори безпеки перевіряють можливість

перехоплення інформації по технічних каналах витоку, і, якщо всі канали надійно захищені, підозра падає на працівників. Діяльність співробітників організації контролюється за допомогою систем обліку робочого часу. [2]

Отже, світ технологій постійно розвивається, потенційні способи вкрасти інформацію у мережі теж розвиваються. Слідування простим правилам може уберегти організацію від великих втрат.

Література:

1. https://www.securitylab.ru/analytics/512440.php—«Что такое «утечка данных» и как предотвратить это.»

2. https://indevlab.com/uk/blog-ua/vitik-danih-br-yak-viyaviti-ta-vipraviti/—«Витік даних: як виявити та виправити?»

ПРИНЦИПИ РОБОТИ І МЕТОДИ ЗАХИСТУ ВІД СКІМЕРІВ ДЛЯ БАНКІВСЬКИХ КАРТ

Лягушкін Іван Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Кіберзлочинці використовують різні методи крадіжки даних про платіжну картку під час транзакції. Щоб краще розібратися в цьому питанні, розглянемо найбільш типові способи, а також заходи захисту, щоб ви не стати жертвою махінацій подібного роду.

Що являє собою скімер платіжної картки

У сфері безпеки під скімером мається на увазі будь-який шкідливий додаток, фізичний пристрій або код, спрямований на крадіжку інформації платіжної картки, в тому числі під час покупок в інтернет-магазинах.

Незалежно від типу скімера (апаратного або програмного) зловмисники переслідують схожі цілі, а конкретно - обман покупця, коли отримана інформація використовується для клонування фізичних платіжних карт або здійснення підроблених транзакцій в інтернеті.

Як працюють скімінгові пристрої

Фізичні скімери проектуються під певні моделі банкоматів, каси самообслуговування і інші платіжні термінали таким чином, щоб ускладнити виявлення. Скімінгові пристрої бувають різних форм, розмірів і мають кілька компонентів.

У кожному скимінгу завжди присутній компонент для зчитування карт, що складається з невеликої мікросхеми, яка живиться від батареї. Зазвичай скімер знаходиться всередині пластикової чи металевої оболонки, що імітує справжній кард-рідер цільового банкомату або іншого пристрою. Цей компонент дозволяє шахраєві скопіювати інформацію, закодовану на

магнітній смузі карти, без блокування реальної транзакції, яку здійснюють користувачем.

Другий компонент скімера - невелика камера, прикріплена до банкомату або підроблена клавіатура для введення пін-коду, що знаходиться поверх справжньої клавіатури. Як неважко здогадатися, мета цього компонента - крадіжка пін-коду, який разом з даними, збереженими на магнітній смузі, використовується для клонування карти і виконання неправомірних транзакцій.

Однак оскільки в багатьох країнах стали використовуватися картки з чіпами, зловмисники також адаптували свої технології і стали виготовляти більш складні скімери. Деякі скімінгові пристрої настільки тонкі, що можуть вставлятися усередину слота карт-рідера. По-іншому ці пристрої називаються скімери глибокого проникнення. Пристрої, які називаються «Шімери» вставляються в слот кард-рідера і спроектовані для зчитування даних з чіпів на картах. Однак слід зазначити, що ця технологія може бути застосована тільки там, де некоректно реалізований стандарт EMV (Europay + MasterCard + VISA).

Програмні скімери

Програмні скімери націлені на програмні компоненти платіжних систем і платформ, будь то операційна система платіжного терміналу або сторінка оплати інтернет-магазину. Будь-який додаток, обробляє незашифровану інформацію про платіжну картку, може стати ціллю для скімінгу.

Як захиститися від скімерів для платіжних карт

Уникайте банкоматів, встановлених поза будівлями або розташованих в місцях з поганим освітленням. Для установки скімерів зловмисники вибирають банкомати в малолюдних місцях, що знаходяться поза банками або магазинів і не під наглядом великої кількості камер.

Перед вставкою карти поворушіть або потягніть кард-рідер і клавіатуру для набору пін-коду і переконайтеся, що ці компоненти не від'єднуються і не зрушуються.

Звертайте увагу на дивні ознаки: отвори, шматки пластики або металу, які виглядають не до місця, компоненти, колір яких не збігається з іншою частиною банкомату і стікери, наклеєні нерівно.

При наборі пін-коду закривайте клавіатуру руками, щоб набрані цифри не змогли потрапити на відео шкідливої камери. Цей метод не допоможе в разі накладної клавіатури, але в цілому скоротить ймовірність крадіжки пін-коду.

Відстежуйте рахунок на предмет неправомірних транзакцій. Якщо у вашій карті передбачені повідомлення через додаток або СМС після кожної транзакції, користуйтеся цими функціями.

Використовуйте дебетову карту, прикріплену до рахунку, де знаходиться невелика кількість грошових коштів, і поповнюйте цей рахунок у міру необхідності, замість використання карти, прикріпленої до основного рахунку, де знаходяться всі ваші гроші.

Отже, світ технологій постійно розвивається, шахраї щоразу знаходять нові способи та методи незаконного збагачення, і постійно треба бути напоготові, щоб не стати їх жертвою. Дотримування простим правилам може уберегти Вас від великих втрат.

Література:

1. https://www.securitylab.ru/analytics/508160.php—« Принципы работы и методы защиты от скиммеров для банковских карт.»

DEVELOPMENT OF ISO REGULATORY BASE IN THE FIELD OF SECURITY INFORMATION TECHNOLOGIES

Мартинюк Михайло Петрович
State University of Telecomunications
Institut of Cybersecurity
Kyiv

The entire world community relies on global information connections, needless to say, the importance of standardizing network protocols, interfaces, and security services and mechanisms. The report provides an overview of some areas of standardization of information technology (IT) security using cryptographic transformations.

1. Structure of ISO committees that develop IT security standards using cryptographic transformations

The following ISO technical committees and subcommittees develop IT security standards:

ISO / IEC JTC 1 Committee “Information Technology”

Subcommittees SC 17 “Identification cards and related facilities”

SC 21 “Open Systems Interconnection”

SC 27 “Safety”

TC 68 Committee “Banking, Securities and Other Financial Services”

Subcommittees SC 2 “Operations and procedures, including

security”

SC 4 “Securities”

SC 6 “Financial transaction cards”

Note that, for example, the SC 4 subcommittee in turn reports to 6 working groups: WG 1, WG 2, WG 3, WG 4, WG 5, WG 6, WG 7. Similarly, many working groups report to other subcommittees.

The above-mentioned structure has both positive features (wide coverage of specialists from different countries, the possibility of independent views on complex issues, etc.) and negative ones: inconsistent terminology, duplication of work in some areas. What measures are taken to eliminate these negative phenomena?

First, there is a lot of painstaking work on standardization of terminology. So at the DIS stage there is a comprehensive dictionary in the field of security. In some of the most vulnerable cases, it is recommended to replace a term or its definition in draft standards.

Second, cross-reference (“subcommittee”) links are used.

Third, attempts are being made to coordinate work.

2. Some features and trends in the development of standards

Of course, in the near future ISO will pay considerable attention to security in e-commerce (business) using the Internet. As stated in SC 27's plenary resolution, the "Internet environment is changing dramatically" due to the growing number of individuals and businesses joining the network. The Organization for Economic Co-operation and Development has set up a special group of experts on "security, protection of private (and intellectual) property in the global information infrastructure", which should develop a strategy for appropriate action.

Here are some features of this question:

– e-business strategy is based on the least interference in existing national (corporate) systems with their platforms, protocols and security systems, ie, frontal standardization on an international scale does not take place;

– the Internet itself does not have the means to acknowledge messages, notarize, etc., the one who transfers funds does not automatically receive any document.

The solution to these problems is partly due to the introduction of special languages for the formation of messages.

Interestingly, the further development of this area by creating a special working group BSR (basic semantic repository) has already been outlined.

Significant difficulties are associated with the integration of security systems in different countries.

References:

1. *https://www.iso.org/structure.html#:~:text=The%20ISO%20Council%20is%20the, Committees%20CASCO%2C%20COPOLCO%20and%20DEVCO.*
2. *International Organization for Standardization - Wikipedia*

AUTOMATION OF THE PROCESS OF INFORMATION SECURITY MANAGEMENT

Наконечний Максим Юрійович
State University of Telecomunications
Institut of Cybersecurity
Kyiv

When organizing the security management system of a modern enterprise, it is necessary to ensure close interaction between employees of information technology divisions and security assurance. The single information space of the enterprise is formed taking into account the need to use its elements for security management. Integrated Security Decision Making Information Support is based on the use of relevant knowledge that accumulates in a single information space.

In order to guarantee the sequence and coherence of the implementation of information security measures, they must be managed. This involves planning, forecasting, evaluating performance and modifications.

In this activity, the collection, processing, analysis and exchange of information is the necessary factor. This occupies the largest part of the information security management process. Even with a small area of implementation of the security system, this is a large amount of work: meetings, interviews, recording the information received, data analysis, developing strategies and corrective measures, developing plans, etc.

In order to automate the processes of data collection, their analysis and interaction, creating of a common information field for all participants in information security processes, an information-logical model of an automated enterprise security management system has been developed.

The following main management processes are distinguished [1]:

- IS incident management;
- implementation of appropriate control mechanisms;
- monitoring the functioning of control mechanisms, evaluating their effectiveness and implementing appropriate corrective actions;
- collection and analysis of data on the state of information security in the organization;
- risk assessment and management;
- development and implementation of protective measures.

These processes can be characterized by a conceptual apparatus in the form of four objects: “threat”, “risk”, “measure”, “remedy” sufficient to build an information security management system (ISMS).

Automation of the control of polarization IS in the maintenance of a database of visits and the accumulation of statistical data through a journal. This database is the main tool for a security specialist, which is used to record work performed. Organizationally, it is necessary to guarantee the work of the security service in such a way that information about all the events carried out and the protective equipment is used are stored in the database.

Based on the previously analyzed control processes, you can depict a diagram communication of objects required for building an ISMS (fig. 1). For each event, the risks worked out are indicated as well as the items that are combined with them. One measure is able to function simultaneously on several risks, reducing the probabilities and losses by all kinds of sizes. For each risk, its initial probability and losses are presented, and also the final ones, taking into account the established measures.

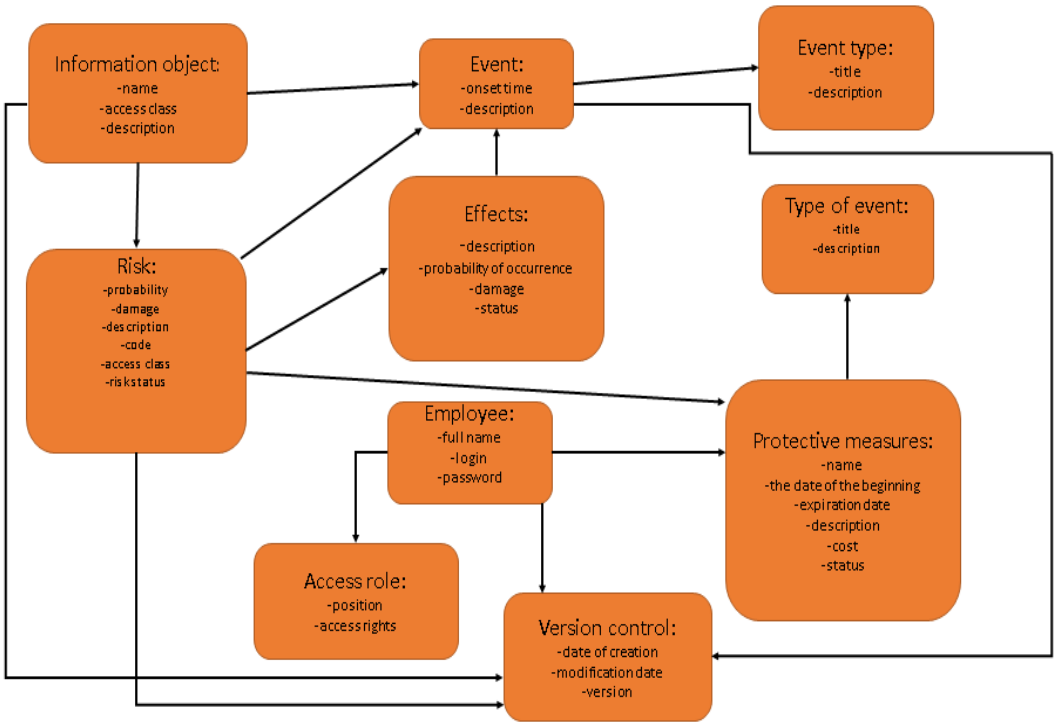


Figure 1. – Unified Modeling Language

The main purpose of the system is to provide the employees of the unit responsible for IS with an event management tool, related to ensuring the security of individual information objects, and to the head of the security unit, which is a tool for monitoring and analyzing risks and evaluating the effectiveness of measures.

References:

1. IEC 27001:2005, Information technology –Security techniques –Information security management systems —Requirements

2. Буч Г, Рамбо Дж., Джекобсон А. UML. Проектирование программных комплексов, информационных систем. – М.: ДМК Пресс, СПб.: Питер, 2003, 432 с.

SECURITY OF INFORMATION IN AUGMENTED REALITY TECHNOLOGY

Наконечний Максим Юрійович
State University of Telecomunications
Institut of Cybersecurity
Kyiv

The rapid growth of the virtual reality market makes the discussion of risks even more relevant. When developing and using mobile applications with augmented reality, it is necessary to take into account possible risks in terms of security and privacy. Existing methods and means of improving security (for example, encryption of data transmitted over wireless channels) can protect input and output information. For this reason it is necessary to have a clear idea of the integration of security tools in the field of augmented reality.

Augmented Reality (AR) is close to realizing the transition to the status of global distribution technology. But, like every other development, augmented reality, along with new features, also carries fresh dangers from the point of view of security. As a result, one needs to have an accurate idea of the integration of security tools into new solutions based on augmented reality technologies. Since augmented reality, along with fresh probabilities, is fraught with risks in terms of security and confidentiality, it is necessary to think about using means of data protection before its application [2].

In contrast to virtual reality, which transfers to the simulated visual world, augmented reality in real time superimposes visual, audio and tactile signals generated by the computer on the natural field of view of a person, as well as an audio and tactile background. This overlay can be navigation data for a car driver, fixing electrical devices schemes, including remote designing of a doctor’s hands during a difficult operation.

If we consider the dangers of augmented reality, the more obvious the distractions will be. For example, too much information in the driver’s field of vision threatens with fatal consequences. The least obvious danger is the penetration of hackers into augmented reality systems with the following penetration into private life, theft of digital data and physical security risks.

However, another scenario is also likely. As augmented reality applications need access to information collected with the support of various sensors, a malicious application has the ability to steal information about the user's field of view or location. For

organizations, in fact, that have not prepared for the impact of augmented reality on the network and security, the risk is much more serious as more and more applications that use augmented reality appear.

In AR applications, the possibilities for malware are almost endless, including keyloggers for capturing user credentials and mobile remote access virus (mobile remote access Virus -mRAT) programs that can infect a device and secretly intercept data and communications, or an agent, via a mobile device loads malware network support. As a result, to ensure control of augmented reality applications in their network is a very important issue for organizations, which is crucial for being proactive and taking necessary protective measures.

In addition, training and awareness raising is of great importance, because human errors and carelessness are often considered to be the main weak spot, used by cybercriminals [4].

The next factor in the AR risk mitigation strategy should be the visibility of application traffic on the network. In order to guarantee protection from exposure to their own secret data or from the introduction of malicious data, firms are required to provide full visibility in real time and understanding of their network traffic throughout the entire time.

References:

1. Горячев А. Защита мобильных приложений от кибератак / Горячев А. // Журнал — InformationSecurity/ Информационная безопасность‖ No4, 2014.

2. Дуайт Дэвис. Реальные риски дополненной реальности / Дуайт Дэвис[Електронний ресурс]. – Режим доступу до ресурсу: http://www.osp.ru/cw/2016/12/13050187/

3. Чому доповнена реальність додає ризику в мережі [Електронний ресурс]. – Режим доступу до ресурсу: http://it-ua.info/news/2016/09/21/chomu-dopovnena-realnst-doda-riziku-merezh.html

4. Sandor C. Immersive mixed-reality configuration of hybrid user interfaces. / C. Sandor, A. Olwal, B. Bell and S. Feiner. // In ISMAR'05, pp. 110–113, 2005.

МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ДИНАМІЧНОГО ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

Наконечний Максим Юрійович
State University of Telecomunications
Institut of Cybersecurity
Kyiv

У роботі проаналізовано метод підвищення безпеки динамічного відеоінформаційного ресурсу в інфокомунікаційних системах, проаналізовано способи запобігання виникненню загроз порушення доступності та цілісності інформації. Ключовим завданням роботи є розробка методу кодування відеоінформаційного потоку для підвищення його безпеки у відомчих

інформаційно-комунікаційних системах на основі структурного опису областей стаціонарного фону, а також представлення методологічних принципів роботи диференційно представлених міжкадрових спектрограм.

Якість функціонування стратегічно значущих для країни галузей багато в чому визначається рівнем інформатизації та забезпечення безпеки інформації. Інформаційна безпека визначається трьома основними категоріями. У тих прикладних сферах діяльності, де критичним є своєчасність і достовірність інформації, найбільшу вагу мають загрози категоріям цілісності і доступності. Прикладом можуть служити системи управління для відомчих організацій [1]. Відеоінформація надходить до центрів аналізу і прийняття рішень.

Від правильності і своєчасності прийнятих рішень залежать як людські життя, так ступінь нанесення економічних збитків державі. Тут існують загрози порушення властивостей доступності і цілісності. Така ситуація трапляється, коли вимоги щодо якості динамічного відеоінформаційного ресурсу призводять до суттєвого зростання інтенсивності, що перевищує пропускну здатність інфокомунікаційних мереж. Для такої ситуації неминучими є затримки по доставці інформації. Для вирішення проблеми, що склалася інтегруються технології обробки зображень [2]. У той же час для існуючих технологій характерні недоліки. Зниження інтенсивності відеопотоку досягається ціною збільшення затримок на час обробки і внесення перекручення інформації. У свою чергу підвищуються ризики втрати її цілісності. Це означає, що тематика досліджень, що стосуються вдосконалення технологій ефективного представлення динамічного відеоінформаційного ресурсу є актуальною.

У той же час структурний аналіз послідовності кадрів зображень показав наявність у них високої надмірності. Ця надмірність обумовлена присутністю в сусідніх кадрах областей стаціонарного фону. Інформацію про стаціонарні області можна передавати використовуючи механізми структурної обробки. Взяття до уваги такої особливості не передбачений для існуючих кодеків відеопотоку. Тому пропонується використовувати підхід, який базується на обробці послідовності кадрів з використанням структурного підходу, що враховує наявність для послідовності кадрів областей стаціонарного фону. Таким чином мета дослідження полягає в розробці методу кодування відеоінформаційного потоку для підвищення його безпеки у відомчих інформаційно-комунікаційних системах на основі структурного опису областей стаціонарного фону. Було створено методологічні принципи ефективного представлення

диференційно представлених міжкадрових спектрограм (ДОС), які базується на тому, що пакети замінюються набором кодів, а кожна ДОС розглядається як рівномірний градієнтна послідовність з локально структурними обмеженнями. Було розроблено метод кодування базових елементів ДОС без втрати інформації по блоковій схемі як процес формування коду відповідного числа в градієнтному базисі.

Література:

1. Баранник В.В., Рябуха Ю.Н. Метод повышения информационной безопасности в системах видеомониторинга кризисных ситуаций: Монография. Черкассы, 2015. 143 с.

2. Баранник В.В., Поляков В.П. Кодирование трансформированных изображений в инфокоммуникационных системах. ХУПС, 2010. – 212 с.

СПОСОБИ ВИЯВЛЕННЯ ІНСАЙДЕРІВ НА ПІДПРИЄМСТВІ

Нечипуренко Ксенія Олександрвіна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Слово «інсайдер», яке використовують по відношенню до співробітника, який краде інформацію в своїй компанії і продає її конкурентам, досить давно і, без сумніву, надовго увійшло в нашу мову. Інформаційна безпека, як відомо, має справу з двома категоріями загроз: зовнішніми і внутрішніми. Саме до останнього типу відносяться інсайдери. Їх діяльність в більшості випадків ненавмисного, і саме тому її важко передбачити і знешкодити. Для цього треба задіяти весь арсенал доступних засобів інформаційної безпеки. Розглянемо типи інсайдерських атак, характеристики, за якими можна відрізнити інсайдера на підприємстві, а також методи запобігання шахрайства та інсайдерства на підприємстві.

Інсайдерські атаки – виток персональної та конфіденційної інформації – серед інших кіберзлочинів мають найвищий рівень латентності (приховування) і найнижчий показник розкриття.

Залежно від ступеня підготовленості «зливу» можна розділити інсайдерські атаки на:

– Ситуативні. Новий співробітник виходить на роботу, у нього є можливість вкрасти, моральні принципи йому це дозволяють, і він робить шахрайство. Або інший приклад: фахівець працює в компанії істотний період, але не отримує належного визнання. Або ж отримує його, але не в тій мірі, на яку розраховував. Природно, працівник не задоволений. Здійснюючи крадіжку інформації, він намагається «компенсувати» собі те, чого, на його думку, був незаслужено позбавлений.

– Сплановані. Найбільш простий приклад - це промислове шпигунство. Про нього відомо більшості сучасних людей з фільмів, книг, рідше - з преси. Менш типовий приклад, коли

співробітник «зливає інформацію» з помсти. Він чітко планує свої дії, він знайомий з тим, як його будуть ловити, знайомий з внутрішніми протоколами безпеки. Такий злочин найскладніше розкрити. [1]

Схильність людини до шахрайства можна виявити, вивчивши його особистісні моральні цінності, особливості прийняття моральних рішень, саморегуляції, визначення його ставлення до себе, інших людей, до праці, до грошей і до норм закону.

Людей, схильних до шахрайства, відрізняють:

– домінування універсальних цінностей, що склалися на основі індивідуалізму і прагматизму;

– жадібне відношення до грошей;

– заперечення значення чесного і продуктивної праці;

– ігнорування традиційних морально-правових норм;

– авантюризм моральної саморегуляції;

– руйнівний цинізм, імпульсивність і схильність до ризику при прийнятті рішень;

– егоїзм. [2]

Високий розвиток цих ознак говорить про психологічну готовність людини до шахрайства. Але важливо пам'ятати і про здорову атмосферу всередині самої компанії.

Що ж потрібно для запобігання шахрайства та інсайда на роботі?

Психологічне тестування, для проведення якого кадрові відділи використовують спеціалізовані програмні продукти, які автоматично аналізують і інтерпретують дані, що значно спрощує процес діагностики.

У загальному вигляді роботу можна будувати за алгоритмом: кадровий відділ проводить тестування при прийомі на роботу або в процесі чергової атестації; дані тестування передаються в службу забезпечення інформаційної безпеки; працівник служби ІБ визначає співробітників, схильних до інсайду; якщо співробітник-володар яскраво вираженого типу, що входить до «групи ризику», то забезпечується першочерговий контроль його діяльності.

Крім цього для захисту від інсайдерської атаки потрібно: чітко окреслити умовно зараховують до групи ризику посади: хто працює з конфіденційною інформацією, персональними даними, документами, що містять комерційну таємницю, тощо; розробити нормативні документи, в яких пояснюється, як працівникам цих посад слід звертатися з конфіденційними даними; визначитися з профілем посади: які компетенції кадровики хотіли або не хотіли б бачити у фахівця на конкретній

позиції; підібрати методики для діагностики морально-психологічних якостей; приймати превентивні заходи: використовуйте рішення для запобігання витоків даних (DLP-системи); впроваджувати політику захисту даних, відстежуючи неавторизоване використання конфіденційної інформації. (Інформування співробітників про порушення допоможе підвищити обізнаність персоналу, утримуючи їх від крадіжки даних); проводити постійну роз'яснювальну роботу: наявність однієї тільки політики, без розуміння і ефективного її застосування співробітниками, не дасть результату; пам'ятати, що крадіжку передують ключові передумови: основні проблеми, пов'язані з мотивацією інсайдера, виникають ще до того, як він здійснює крадіжку; мати на увазі, що співробітника можуть «підштовхувати до дії» інші працівники. Це часто відбувається в разі зниження по службі або коли кар'єрні очікування не виправдовуються; домогтися інформування керівництва, HR-відділу і персоналу, що відповідає за інформаційну безпеку, про всі випадки, коли діючий або звільнений співробітник звертається до критично важливих даних, завантажує їх нетиповим чином тощо. [3]

Отже, дотримуючись цих правил, можна в значній мірі убезпечити себе і свою компанію від перетворення людей, потенційно схильних до інсайду, в повноцінних інсайдерів.

Література:

1. Инсайдеры: такие разные и такие похожие! [Електронний ресурс] // SecurityLab. – 2018. – Режим доступу до ресурсу: https://www.securitylab.ru/blog/company/securityinform/113284.php.

2. Астахов А. Как защищаться от инсайдера? [Електронний ресурс] / Александр Астахов // ISO27000. – 2017. – Режим доступу до ресурсу: http://iso27000.ru/chitalnyi-zai/zaschita-ot-insaiderov/kak-zaschischatsya-ot-insaidera.

3. ВЫЯВЛЕНИЕ ИНСАЙДЕРА [Електронний ресурс] // СёрчИнформ КИБ. – 2019. – Режим доступу до ресурсу: https://searchinform.ru/resheniya/biznes-zadachi/vyyavlenie-insajdera/.

МЕТОДИ ОЦІНКИ АКТУАЛЬНИХ ЗАГРОЗ ТА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Нощенко Станіслав Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

З розвитком сучасних технологій і електронної комерції з кожним днем з'являється все більше загроз безпеки інформації. Сьогодні організації все частіше використовують інформацію в бізнес-процесах, для полегшення управлінських рішень і ведення бізнесу. Така інформаційна залежність привела до істотного збільшення впливу рівня безпеки інформаційних систем на успіх, а

іноді і просто можливість ведення бізнесу. Тому безпека інформаційних систем є одним з найважливіших питань, яке привертає велику увагу з боку аналітиків, інженерів та інших фахівців в області інформаційно безпеки.

В загальному в світі існує кілька десятків різного роду методик і підходів до оцінки ризиків ІБ, таких як: Austrian IT Security Handbook, AS / NZS4360, BSI 100-3, CRISAM, EBIOS, HB167: 200X, ISF IRAM, CRAMM, ISO 27005, MAGERIT, MARION, MEHARI, NIST SP800-30, OCTAVE, OSSTMMRAV, SOMAP та інші, але частина з них вже застаріла і не розвивається, частина не володіє актуальними перекладами на англійську мову з мови країни походження, що робить складним їх вивчення для широкої аудиторії. В даній роботі будуть розглянуті саме ті методики, які містять розгорнутий підхід, досить широко відомі в Україні і продовжують розвиватися (або ще не втратили своєї актуальності) і відносно легко доступні. Вибір тієї чи іншої методики залежить від рівня вимог, що ставить перед собою підприємство до забезпечення безпеки інформації, характеру загроз, що беруться до уваги, і ефективності контрольних заходів щодо захисту інформації.

ISO 27005 - це стандарт із серії 2700x, що описує підхід до організації всього процесу з управління ризиками інформаційної безпеки. Представлена в стандарті методика оцінки є класичною і має за недоліки зайву академічність і загальність формулювань. Даний стандарт описує настанови і рекомендується до ознайомлення з метою формування загального уявлення про організацію процесу з управління ризиками ІБ.

В NIST SP800-30 представлені підходи не тільки до оцінки ризиків, а й до організації діяльності з управління ризиками інформаційної безпеки на різних рівнях (від стратегічного до прикладного на рівні окремих інформаційних систем). На відміну від ISO 27005 даний документ містить більш розгорнуті описи кожного з елементів, а також рекомендації щодо застосування на практиці в різних ситуаціях.

Методика NIST SP800-30 передбачає попереднє оцінювання двох параметрів: потенційного збитку і ймовірності реалізації загрози. Застосування системи управління ризиками безпосередньо пов’язано з можливістю підприємств виконувати свої основні функції в умовах постійного розширення сфери використання інформаційних технологій.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика проведення оцінки ризиків в організації, що була розроблена інститутом Software Engineering Institute (SEI) при університеті Карнегі Меллон (Carnegie Mellon University). Цей підхід був створений, щоб допомогти

організаціям ідентифікувати і оцінити ризики інформаційних систем, поліпшити їх можливості і захистити себе від цих ризиків. Особливість даної методики полягає в тому, що весь процес аналізу проводиться силами співробітників організації, без залучення зовнішніх консультантів. Для цього створюється спільна група, що включає як технічних фахівців, так і керівників різного рівня, що дозволяє всебічно оцінити наслідки для бізнесу можливих інцидентів в області безпеки і розробити контрзаходи.

Інструментальні засоби аналізу ризиків дозволяють автоматизувати роботу спеціалістів в області захисту інформації, які здійснюють оцінку або переоцінку інформаційних ризиків підприємства.

Спеціалізоване ПЗ, що реалізує методики аналізу ризиків, може відноситись до категорії програмних продуктів (продається на ринку) або бути власністю відомства або організації і не продаватися. Якщо ПЗ розробляється як програмний продукт, воно повинно бути в достатній мірі універсальним. Відомчі варіанти ПЗ адаптовані під особливості постановок задач аналізу та управління ризиками, і дозволяють врахувати специфіку інформаційних технологій організації.

Пропоноване на ринку ПЗ орієнтоване в основному на рівень інформаційної безпеки, який трохи перевищує базовий рівень захищеності. У 2005 році був прийнятий міжнародний стандарт ISO / IEC 27001, за основу якого було взято Британський стандарт BS 7799. В результаті більшість інструментальних засобів (ПЗ аналізу ризику) було останнім часом модифіковано таким чином, щоб забезпечити відповідність вимогам саме цього стандарту. Спеціалізоване ПЗ умовно можна розділити на дві групи: ПЗ базового рівня і ПЗ повного аналізу ризиків.

Для розв'язання задачі оцінки ризиків інформаційної безпеки в даний час найбільш часто використовуються наступні програмні комплекси: CRAMM, FRAP, RiskWatch, Microsoft Security Assessment Tool (MSAT), CORAS і ряд інших.

Література:

1. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки.

2. Information security. National Institute of Standards and Technology. 2012.

3. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process [Текст] / R. A.Caralli, J. F. Stevens, L. R. Young, L. R. Wilson.– Бостон: Університет Карнегі-Меллон, 2007. – 0.3354 с

МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ «СИСТЕМИ РОЗУМНИЙ ДІМ» НА БАЗІ НОВОГО ПРОТОКОЛУ ОБМІНУ ДАНИХ

Овчиннік Сергій Олександрович, Лаптєв Олександр Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Сьогодні, завдяки нестримному розвитку мікроелектроніки, каналів зв'язку, Інтернет-технологій і Штучного Інтелекту, тема «розумних будинків» стає все більш і більш актуальною. Людське житло зазнало істотних змін з часів кам'яного віку і в епоху Промислової Революції 4.0 і Інтернету Речей стало зручним, функціональним і безпечним.

Розумний будинок включає в себе величезну кількість IoT-пристроїв, які збирають і обробляють дані. Вони дають користувачам певні можливості по контролю за апартаментами як в ручному, так і автоматичному режимі. У «розумному середовищі» пристрої періодично обмінюються даними по мережі. Це відбувається або безпосередньо від пристрою до пристрою, або через хмару. Тому захист передачі інформації клієнт-«розумний будинок» є дуже актуальним на сьогоднішній день.

Особливістю роботи - «розумного будинка» є те, що більшість команд на пристрої проходять через мережи передачі даних. В цілому всі елементи ланцюжка мають доступ в Інтернет. Це робить їх уразливими до атак ззовні і наражає на небезпеку не тільки інформацію користувача, але також його здоров'я. Все це змінює парадигму мислення, в якій мовиться: «Мій будинок - острівець безпеки».

Однак безпека, особливо безпека протоколів обміну даними між клієнтом та «розумний будинок» - це 100% вимога для розумного будинку. До складу системи безпеки можуть входити системи спостереження, системи моніторингу (в тому числі здоров'я) і системи безпеки, до яких можна отримати віддалений доступ.

Компанія HP провела дослідження ринку інтелектуальних систем в ході якого з'ясувала, що практично всі системи мають проблеми з безпекою.

Перша проблема - недостатньо надійна перевірка аутентифікації. Системи, незважаючи на те, що володіли хмарними і мобільними інтерфейсами, не вимагали установки паролів достатньої довжини і складності. Жодна з систем не блокувала обліковий запис після певного числа невдалих спроб введення пароля.

Ще одна проблема виявилася пов'язана з конфіденційністю. Всі системи збирали будь-які види персональної інформації: імена, адреси, номери телефонів і

кредитних карт. Це викликає певну стурбованість, оскільки створює загрозу крадіжки облікових даних.

Варто також відзначити, що ключовою особливістю багатьох домашніх систем безпеки є використання відео, перегляд якого доступний через різні інтерфейси. Конфіденційність подібних даних теж знаходиться під питанням.

Нарешті, останньою проблемою експерти назвали відсутність шифрування при передачі даних. Хоча у всіх системах реалізовані механізми шифрування на транспортному рівні, такі як SSL / TLS, багато хмарні підключення залишаються уразливими для атак.

Дуже важливий момент: щоб виключити несанкціоноване втручання в роботу пристрою, обмін між контролером і сервером повинен йти в зашифрованому вигляді. Для забезпечення безпеки протоколів обміну даних потрібно відволіктися від основної функції техніки і почати сприймати її як комп'ютерну мережу, щоб помітити дірки в інформаційній безпеці.

Таким чином, компанії Google, Samsung Electronics, Silicon Labs і деякі інші об'єдналися з метою розробити новий бездротовий мережевий стандарт спеціально для розумних будинків. Він отримав назву Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основним його достоїнством є саме безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи.

Ще одна особливість Thread - це прозорість. Користувач бачить список всіх підключених пристроїв, завдяки якому йому легко визначити, що з чим пов'язано. На даний момент є ряд рішень для розумних будинків (ZigBee і 6LowPAN), які легко можуть почати підтримувати запропонований стандарт без апаратних змін - в їхньому випадку потрібно просто оновити програмне забезпечення.

Цей сценарій показує, наскільки глибоко IoT став інтегруватися в життя людей. Це очевидно з того, як існує застосований пристрій IoT для кожної частини будинку, від вітальні і кухні до ванної кімнати і горища. Ця глибока участь в житті людей робить атаки Інтернету речей життєздатними для хакерів і ефективними для користувачів. Можливо, ніде кіберзагрози більш не були потенційно агресивними і особистими, ніж в розумних будинках.

Але нам пропонується удосконалення цього стандарту.

Пропонується модифікація відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих криптографічних закладок та підвищення криптостійкості в постквантовий період (поява повномасштабного квантового комп'ютер, що дозволяє зламати на основі алгоритмів Гровера та Шора сучасні симетричні та асиметричні криптосистеми). Крім того, комерційне впровадження забезпечить "протидію" можливих криптодепозитів спецслужбами, що зменшить ризик злому шляхом виявлення "слабких" (вразливих) місць на основі криптографічних закладок.

В алгоритмі блок, що шифрується (довжина 64 біта), розділений на дві рівні частини (32 біти) - праву та ліву. Далі тридцять дві ітерації виконуються з використанням ітераційних ключів, отриманих з вихідного 256-бітного ключа шифрування. Під час кожної ітерації здійснюється одне перетворення на основі мережі Фейстела з правою та лівою половиною зашифрованого блоку. Спочатку права частина складається в модуль 232 з поточним ітераційним ключем, потім отримане 32-бітове число ділиться на вісім 4-бітових і кожен з них, використовуючи таблицю перестановок, перетворюється в інший 4-бітний номер. Після цього перетворення отримане число крутиться вліво на одинадцять розрядів. Далі XOR трансформується з лівою половиною блоку. Отримане 32-бітове число записується в правій половині блоку, а старий вміст правої половини переноситься в ліву половину блоку. Такий алгоритм захисту значно покращить захист переданої інформації клієнт - «розумний будинок».

Окрім математично технічних засобів розроблені практичні рекомендації щодо захисту пристроїв IoT у своїх розумних будинках. Заходи безпеки, які користувачі можуть прийняти для захисту своїх розумних будинків від атак на пристрої Інтернету речей:

1) **Зрівняйте всі підключені пристрої**. Всі пристрої, підключені до мережі, наприклад, вдома чи на рівні підприємства, повинні бути добре враховані. Слід зазначити їх налаштування, облікові дані, версії прошивки і останні виправлення. Цей крок може допомогти оцінити, які заходи безпеки слід вжити користувачам, і визначити, які пристрої, можливо, доведеться замінити або оновити.

2) **Змініть паролі та налаштування за замовчуванням**. Переконайтеся, що установки, що використовуються кожним пристроєм, відповідають більш високої безпеки, і поміняйте налаштування, якщо це не так. Змініть паролі за замовчуванням

і слабкі паролі, щоб уникнути атак, таких як груба сила і небажаний доступ.

3) **Патч вразливостей**. Установка виправлень може виявитися складним завданням, особливо для підприємств. Але обов'язково застосовувати виправлення відразу після їх випуску. Для деяких користувачів виправлення можуть порушити їх звичайні процеси, для чого можна використовувати віртуальне виправлення.

4) **Застосовуйте сегментацію мережі**. Використовуйте сегментацію мережі, щоб запобігти поширенню атак і ізолювати потенційно проблемні пристрої, які не можна відразу відключити.

Висновок

Проведений аналіз проблем безпеки обміну даними між клієнт - «розумний будинок». Визначені пріоритети захисту інформації на етапі передачі інформації. Проведений аналіз запропонованого нового бездротового мережевого стандарту Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основним його достоїнством є безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Але цього недостатньо для забезпечення цілісності інформації.

Запропоновано використання нового алгоритму шифрування на основі поточного алгоритму шифрування, заснованого на алгоритмі блокчейну, завдяки використанню динамічно змінюваного нелінійного бієктивного перетворення (S-блоки) дозволяє уникнути значних проблем інформаційної безпеки.

Цей алгоритм використовуються для забезпечення конфіденційності (безпеки під час передачі), цілісності (безпеки при зберіганні та модифікації лише для авторизованих користувачів) та автентичності (достовірність джерела повідомлення). Та забезпечує надійний захист інформації.

Підсумовуючи етапи захищеності, знайдемо «Підвищення ймовірності захищеності»:

Нехай, існує захищеність з ймовірністю P1. P1 – це стандартний захист «розумного дому». Але, як виявилося, алгоритми шифрування і конфіденційність даних була на проблематичному рівні. Постає питання покращити безпеку, розробивши бездротовий мережевий стандарт, ймовірність якого P2. Тепер існує ймовірність захищеності P1+P2. Згадавши, що в системах «Розумний дім» відсутнє шифрування, запропонуємо модифікацію відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих

криптографічних закладок та підвищення криптостійкості в постквантовий період, ймовірність захищеності якого P3. Разом з цим ймовірність захищеності P1+P2+P3. Загальна система виглядатиме так: P=P1+P2+P3. Для прикладу, P1=0.4, P2=0.25, P3=0.3. Тоді загальна ймовірність захищеності системи P=0.95

Література:

1. IoT: Вопросы безопасности умного дома. URL: https://habr.com/ru/company/gsgroup/blog/394343/ (дата звернення: 10.10.2020)

2. Inside the Smart Home: IoT Device Threats and Attack Scenarios. URL: https://www.trendmicro.com/vinfo/gb/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios (дата звернення: 10.10.2020)

3. Security and privacy issues for an IoT based smart home. URL: https://ieeexplore.ieee.org/document/7973622 (дата звернення: 10.10.2020)

4. How safe are smart homes?? URL: https://www.kaspersky.com/resource-center/threats/how-safe-is-your-smart-home (дата звернення: 10.10.2020)

5. Encryption algorithm GOST 28147 89 c. GOST architecture notes. URL: https://newtravelers.ru/en/nastrojjka/algoritm-shifrovaniya-gost-28147-89-c-zamechaniya-po-arhitekture.html (дата звернення 14.10.2020)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖІ КОРПОРАТИВНИХ ПІДПРИЄМСТВ

Олійник Є. О.
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Захист локальної мережі є нагальною потребою будь-якої організації. Вдосконалення засобів та методів, що використовують зловмисники, з кожним днем підвищують вразливість інформації. Більшість корпоративних компаній мають розгалужену і розподілену мережеву інфраструктуру, при цьому кількість мережевого трафіку стає настільки великою, що контролювати його будь-яким чином і аналізувати стає складним завданням, особливо щоб забезпечити належний рівень інформаційної безпеки.

Одним із засобів забезпечення безпеки мережі є моніторинг. На сьогоднішній день відомо безліч способів моніторингу мережі. Наприклад, методи, засновані на маршрутизаторах, а саме:

• SNMP – протокол, який є частиною TCP / IP. Дає можливість адміністраторам налаштовувати продуктивність мережі, усувати проблеми, стежити за зростанням мережі. Є можливість збирати статистику;

• RMON (Remote Monitoring) – має безліч мережевих моніторів і систем для зміни даних, отриманих в результаті моніторингу мережі;

• Netflow – розширення, доступні в маршрутизаторах Cisco, що надають можливість відстежувати мережевий трафік.

Такі методи сильно зав'язані на самих маршрутизаторах і мають погану гнучкість, тому краще [1] використовувати наступні методи. А саме:

• активний моніторинг, який повідомляє проблеми в мережі, збираючи дані між двома мережевими точками. Додає трафік в мережу і може змінювати трафік в самій мережі;

• пасивний моніторинг, який збирає інформацію з однієї мережевої точки. Не змінює трафік в мережі;

• комбінований моніторинг – це поєднання активного і пасивного моніторингу, що є найкращим варіантом [2].

При цьому лише одного моніторингу для забезпечення безпеки мережі недостатньо. Адже проаналізувати вручну особливо велику кількість мережевого трафіку неможливо. Тут на допомогу приходять системи виявлення вторгнень (СВВ). Системи виявлення й запобігання вторгнень призначені для постійного моніторингу корпоративної мережі, а також виявлення та виявлення атак [3]. Переваги даних рішень наступні:

• покриття моніторингу мережі і повний контроль трафіку;

• декілька оптимально розташованих систем виявлення вторгнень можуть здійснювати моніторинг дуже навантажених мереж;

• відсутність впливу на продуктивність мережі в цілому;

• отримання інформації про проникненнях в систему;

• визначення джерела атаки;

• прогнозування можливих атак.

Серед недоліків можна виділити наступні:

• потрібна додаткове налаштування мережевих пристроїв, а також додаткових мережевих ресурсів;

• неможливість аналізу зашифрованої інформації;

• деякі рішення дуже важкі в налаштуванні, експлуатації та аналізі отриманих даних.

СВВ, що найчастіше використовуються, є мережеві (Network Based IDS) і хостові (Host Based IDS). Нижче докладніше розглянемо їх особливості, можливості і недоліки [4].

Мережеві СВВ не мають можливості розпізнавати результат атаки (чи була вона успішною чи ні), вони лише знають про те, що атака була ініційована.

Хостові СВВ агрегують дані з одного хоста, що дозволяє аналізувати точну інформацію, визначаючи дані, що мають відношення до конкретної операційної системи. В основному

використовують результати аудиту операційної системи, логи системи, події безпеки.

Переваги: можливість стежити тільки за подіями хоста, визначаючи атаки, не видимі для мережевих СВВ; не вимагають додаткового налаштування мережевих пристроїв.

Недоліки: досить важкі в управлінні, оскільки повинні бути налаштовані для кожного окремого хоста; можуть бути блоковані з допомогою DDOS атак; спричиняють сильний вплив на продуктивність системи.

Таким чином, на основі короткого аналізу показано, що на даний момент найкращим варіантом СВВ буде гібридна СВВ, що включає в себе: аналіз мережі на основі поведінки користувачів або хостів, виявлення відомого спектра атак; систему нотифікацій (смс, email повідомлення); відсутність складного налаштування системи, як наприклад СВВ, засновані на сигнатурних методах виявлення, коли потрібно налаштовувати велику кількість правил; здатність знаходити невідомі раніше типи атак на основі машинного вивчення.

Отже, з усього вищезазначеного можна зробити висновок, що використання засобів моніторингу та СВВ разом дозволить вивести інформаційну безпеку корпоративних компаній на абсолютно новий рівень, оскільки швидке реагування на виконану в реальному часі атаку, що завдає загрозу даним компанії, дасть можливість знизити матеріальні втрати.

Література:

1. Alicia Cecil. A Summary of Network Traffic Monitoring and Analysis Techniques / Alicia Cecil. – URL: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html

2. Рассел, Джесси. Система обнаружения вторжений / Джесси Рассел. – М., 2012.

3. Норткатт, Стивен. Обнаружение вторжений в сеть: настольная книга специалиста по системному анализу / Стивен Норткатт, Джуди Новак. – М.: Лори. 2001.

4. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. – М.: Горячая линия-Телеком, 2013.

ДАКТИЛОСКОПІЧНИЙ МЕТОД У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Панченко Максим Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Одним з напрямків захисту інформаційних систем є оснащення приміщень з комп'ютерною технікою і процедур відкриття програмних засобів та баз даних пристроями доступу. У статті розглянуто властивості дактилоскопічного методу ідентифікації особи та величини параметрів FAR і

FRR для різних типів систем доступу. Запропоновано рекомендації щодо напрямків застосування цих методів у системах захисту інформації.

У теперішній час методи ідентифікації з використанням «ручного» набору паролю замінюються на більш надійні: пластикові беджі, смарт – карти з введенням додаткового паролю, «інтелектуальні» картки з мікрочіпом, тощо. Ці засоби характеризуються набагато вищим ступенем захисту від підбору, копіювання, фальсифікації ключових даних по-рівняно з ручним вводом. Але всі карткові методи мають принциповий недолік – перевіряється перетинання рубежу захисту предметом ідентифікації, а не особою, яка має право доступу. При цьому картка може бути викрадена, загублена, підроблена, пере-дана, тощо.

Єдиним беззаперечним способом ідентифікації на сьогодні є виявлення за допомогою технічних пристроїв біологічних характеристик особи та перевірка їх відповідності заздалегідь сформованим особистим шаблонам. Біометрика (англ. Biometrics) – це методи ідентифікації особи, що використовують фізіологічні параметри людини – відбитки пальців або долоні, зображення обличчя, рай дужну оболонку або сітківку ока, голос, ДНК, тощо. Використання цих технологій має певну історію, а їх «друге народження» почалось після відомих терористичних атак 11 вересня 2001 р. Результатами стали бурхливий розвиток біометричних технологій та їх широке впровадження у системи безпеки різноманітного призначення. Відбулося значне здешевлення такої апаратури при підвищенні безпомилковості її роботи. Звичайно біометричні методи розділяють на статичні, коли відповідні ознаки особи практично не змінюються у часі, та динамічні, які використовують дані про особливості поведінки людини. Для систем захисту інформації цінність представляють в основному статичні методи, що фіксують незмінні характеристики особи, притаманні їй від народження.

Дактилоскопічний метод базується на унікальності та незмінності протягом життя відбитків пальців людини, що доведено криміналістичною наукою та підтверджено експертною практикою. На відбитку пальця знаходяться мінуції – унікальні для кожного узору точки зміни структури папілярних ліній – їх закінчення, роздвоєння, розрив, тощо. Система визначає для кожної мінуції її координати і орієнтацію папілярних ліній у цій точці. Еталонний відбиток містить приблизно 70 мінуцій.

Для оцінки якості біометричних систем ідентифікації введено такі характеристики:–імовірність допуску особи, яка не

має права доступу (False Acceptance Rate - FAR), це найбільш небажаний результат, який повинен бути мінімізованим; –імовірність відмови особі, яка має право до-ступу (False Rejection Rate - FRR), такий помилко-вий результат можна виправити. Ці характеристики взаємопов'язані – чим менше одна, тим більше друга. Точка, у якій ці дві помилки рівні, називається EER (Equal Error Rates). Чим менша величина EER , тим вище безпомилковість системи доступ

Дактилоскопічний метод розпізнання займає приблизно половину ринку систем доступу. Достатньо вказати, що майже третина сучасних ноутбуків оснащена вбудованою системою зчитування відбитків пальця, такі датчики вмонтовують у клавіатури ПК, Миші, флеш - накопичувачі, замки дверей, тощо.

Термін ідентифікації відбитку дактосистемою коливається від 0,5 до 5 сек., звичайно це припустима величина. Можна відмітити, що датчик найбільш якісної системи No4 виробляється на Чернігівському заводі радіоприладів, Україна. Реальні показники якості систем можуть погіршуватись у процесі експлуатації через забруднення датчика чи пальця, або через слабко виражені папілярні узори у людей фізичної праці, або через пошкодження пальця (іноді умисні), тощо.

Треба констатувати розповсюдженість думки про легкість створення дактилоскопічного муляжу та обману таких систем. У джерелах описаний експеримент спеціаліста по безпеці з університету Йокогами (Японія) Цутому Мацумото (Tsutomu Matsumoto). Він виготовив муляж пальця , за допомогою якого у 2002 р. на кількох різних сканерах одержав вірогідність помилкового допуску FAR у 70-95%, що є вкрай негативним. Також описаний експеримент з протилежним результатом, проведений після 2004 р. компанією «Ревер», Москва. Муляж власноручного виготовлення перевірявся на трьох сканерах та на миші з дактилоскопічним датчиком. У серіях по 100 спроб ні одна з трьох систем не сприйняла підроблений муляж у як ості відбитка пальця. Тільки датчик миші один раз за серію зчитав фальшивий відбиток, але при ідентифікації його з еталонним записом у базі даних система дала відмову у доступі. Для протидії муляжам тепер успішно використовують сканери, які додатково реагують на температуру, пульс, вологість живого пальця.

Література:

1. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомунікаційних систем

2. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем.

3. Лисенко А.М., Мельник О.С. Застосування біометричних систем для ідентифікації особи

ОСНОВНІ ЗАХИСНІ МЕХАНІЗМИ ОС РЯДУ UNIX

Панченко Максим Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

На сьогоднішній день існує досить велика статистика загроз ОС, спрямованих на подолання вбудованих в ОС механізмів захисту, які дозволяють змінити налаштування механізмів безпеки, обійти розмежування доступу і т.д. Таким чином, статистика фактів несанкціонованого доступу до інформації показує, що більшість поширених систем (універсального призначення) досить вразливі з точки зору безпеки. І це незважаючи на виразну тенденцію до підвищення рівня захищеності цих систем. У цій статті розглянемо операційні системи ряду UNIX та виявимо суттєві недоліки її захисних механізмів.

Захист ОС ряду Unix у загальному випадку базується на трьох основних механізмах:

1) ідентифікації та аутентифікація користувача при вході в систему;

2) розмежуванні прав доступу до файлової системи, в основі якої знаходиться реалізація дискреційної моделі доступу;

3) аудит, тобто реєстрація подій. При цьому відзначимо, що для різних клонів ОС ряду Unix можливості механізмів захисту можуть незначно відрізнятися, проте будемо розглядати ОС Unix у загальному випадку, без урахування деяких незначних особливостей окремих ОС цього ряду.

Побудова файлової системи і розмежування доступу до файлових об'єктів має особливості, притаманні даному ряду ОС. Розглянемо коротко ці особливості. Всі дискові накопичувачі (томи) об'єднуються в єдину віртуальну файлову систему шляхом операції монтування тому. При цьому вміст тому проектується на вибраний каталог файлової системи. Елементами файлової системи є також всі пристрої, що вмикаються до комп'ютера, який захищається (монтовані до файлової системи). Тому розмежування доступу до них здійснюється через файлову систему.

Кожний файловий об'єкт має індексний дескриптор, в якому серед іншого зберігається інформація про розмежування доступу до даного файлового об'єкту. Права доступу діляться на три категорії: доступ для власника, доступ для групи і доступ для інших користувачів. У кожній категорії визначаються права на читання, запис і виконання (у випадку каталогу - перегляд).Користувач має унікальний символьний ідентифікатор (ім'я) і числовий ідентифікатор (UID). Символьний ідентифікатор пред'являється користувачем при

вході в систему, числовий використовується операційною системою для визначення прав користувача у системі (доступ до файлів тощо).

Принципові недоліки захисних механізмів ОС ряду Unix. Розглянемо в загальному випадку недоліки реалізації системи захисту ОС ряду Unix у частині невиконання вимог до захисту конфіденційної інформації, безпосередньо пов'язаних із можливістю несанкціонованого доступу до інформації. Для початку зазначимо, що в ОС ряду Unix внаслідок реалізованої нею концепції адміністрування (не централізованої) неможливо забезпечити замкнутість (або цілісність) програмного середовища. Це пов'язано з неможливістю встановлення атрибуту "виконання" на каталог (для каталогу даний атрибут обмежує можливість "огляду" вмісту каталогу). Тому при розмежуванні адміністратором доступу користувачів до каталогів користувач, як "власник" створюваного ним файлу, може занести у свій каталог виконуваний файл і, як його "власник", встановити на файл атрибут "виконання", після чого завантажити записану ним програму. Ця проблема безпосередньо пов'язана з реалізованою в ОС концепцією захисту інформації.

Не в повному обсязі реалізується дискреційна модель доступу, зокрема, не можуть розмежовуватися права доступу для користувача "root" (UID=0), тобто даний суб'єкт доступу виключається зі схеми управління доступом до ресурсів. Відповідно всі процеси, які запускаються, мають необмежений доступ до ресурсів, що захищаються. З цим недоліком системи захисту пов'язана множина а так, зокрема:

-несанкціоноване одержання прав root;

-запуск із правами root власного виконуваного файлу (локально чи віддалено впровадженого), при цьому несанкціонована програма одержує повний доступ до ресурсів, що захищаються, тощо.

Крім того, в ОС ряду Unix неможливо вбудованими засобами гарантовано видаляти залишкову інформацію. Для цього в системі абсолютно відсутні відповідні механізми.

Необхідно також відзначити, що більшість ОС даного ряду не мають можливості контролю цілісності файлової системи, тобто не містять відповідних вбудованих засобів. У кращому випадку додатковими утилітами може бути реалізований контроль конфігураційних файлів ОС за розкладом у той час, як найважливішою можливістю даного механізму можна вважати контроль цілісності програм (застосувань) перед їх запуском, контроль файлів даних користувача і т.д.

Що стосується реєстрації (аудиту), то в ОС ряду Unix не забезпечується реєстрація видачі документів на "тверду копію", а також деякі інші вимоги до реєстрації подій. Якщо ж трактувати вимоги до управління доступом у загальному випадку, то при захисті комп'ютера в складі ЛОМ необхідне управління доступом до вузлів мережі. Проте вбудованими засобами в деяких ОС ряду Unix управління доступом до вузлів не реалізується.

З наведеного аналізу видно, що чимало механізмів, необхідних із точки зору виконання формалізованих вимог, більшістю ОС ряду Unix не реалізується в принципі, або реалізується лише частково.

Література:

1. *Струков В.М.Комп'ютерні основи систем кібербезпеки*
2. *Барановская Т.П. Архитектура компьютерных систем и сетей*

ДОСЛІДЖЕННЯ ШЛЯХІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ В ХМАРНОМУ СЕРЕДОВИЩІ НА БАЗІ РІШЕНЬ AMAZON WEB SERVICES

Поремський Максим Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Разом з розвитком інформаційних технологій все більшої популярності набувають рішення на базі хмарних обчислень. Згідно з щорічним звітом Right Scale про стан хмарних обчислень за 2019 рік, 91% підприємств використовували публічні хмарні обчислення, а 72% - приватні. Більшість підприємств фактично використовують обидва варіанти - 69% з них обирають гібридне хмарне рішення [1]. З підвищенням популярності хмарних обчислень, питання забезпечення їх кібербезпеки стають більш актуальним.

Для визначення загроз для хмарного середовища, можно звернутись до матриць ATT&CK. MITER ATT&CK - це загальнодоступна база знань тактики та техніки зловмисника, заснована на реальних спостереженнях. База знань ATT&CK використовується як основа для розробки конкретних моделей та методологій загроз [2]. Безпека - це практика захисту інтелектуальної власності від несанкціонованого доступу, використання або модифікації. Amazon Web Services (AWS) надає декілька послуг, які можна використовувати для того, щоб покрити описані речі та загрози, що наведені в матриці ATT&CK.

AWS використовує модель спільної відповідальності, коли AWS відповідає за захист глобальної інфраструктури, яка

запускає всі послуги, пропоновані в AWS. Ця інфраструктура включає апаратне забезпечення, програмне забезпечення, мережі та засоби, що працюють із службами AWS. Клієнт AWS відповідає за захист своїх даних, операційних систем, мереж, платформ та інших ресурсів, які він створює в хмарі AWS. Він відповідає за захист конфіденційності, цілісності та доступності своїх даних, а також за дотримання будь-яких конкретних стандартів, таких як PCI DSS. Ця модель зображена на рис. 1.

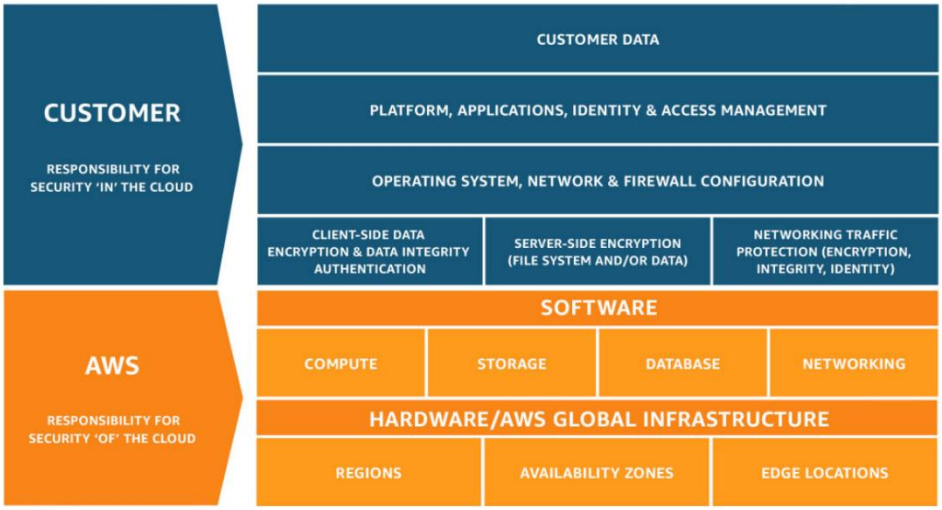


Рис. 1. Модель спільної відповідальності

Сервіси AWS для забезпечення кібербезпеки можна поділити на декілька категорій, кожна з яких вирішує набір задач, завдяки існуючим сервісам:

- Identity and access management (Amazon Cognito, AWS Directory Service, AWS Identity and Access Management, AWS Single Sign-On)
- Detective controls (AWS Security Hub, Amazon GuardDuty, Amazon Inspector, Amazon Detective, Amazon Macie)
- Infrastructure protection (AWS Shield, AWS WAF, AWS Firewall Manager)
- Data protection (AWS KMS, CloudHSM, ACM, Secrets Manager)
- Incident response (AWS Config)

Наведений перелік сервісів дозволяє відповідати на вимоги стандартів з кібербезпеки, а також допомагає в усуненні загроз для хмарних обчислень.

Отже, швидкий розвиток та перехід в нові середовища, змінив ландшафт загроз кібербезпеки, але індустрія швидко реагує на нові виклики та створює рішення, щоб бути в змозі відповідати вимогам стандартів з кібербезпеки та підтримувати її на належному рівні.

Література:

1. Right Scale's annual State of the Cloud Report for 2019 [Електронний ресурс] – Режим доступу до ресурсу: https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf.

2. MITRE ATT&CKO: Design and Philosophy [Електронний ресурс] – Режим доступу до ресурсу: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

СОЦІАЛЬНА ІНЖЕНЕРІЯ

Потапенко Антон Юрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Комп'ютерна безпека *— це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.*

Кібербезпека *— захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі*

Безпека мобільних додатків

Мільйони людей по всьому світу користуються мобільними пристроями і стільки ж людей користуються різними додатками, користуються мобільним інтернетом і браузерами.

Розробка мобільних додатків в тренді, її технології безперервно розвиваються. Більшість сучасних рішень мають клієнт-серверну архітектуру. Клієнт працює під управлінням мобільної операційної системи; найчастіше це Android або iOS. Клієнтська частина завантажується на пристрій з так званого магазину додатків - спеціалізованої майданчика, де розробники розміщують свої системи. З точки зору звичайного користувача, встановлена на смартфон програма - це і є мобільний додаток, адже саме з нею він взаємодіє безпосередньо: здійснює покупки, оплачує рахунки, переглядає пошту. Але в дійсності є ще один компонент, який прийнято називати сервером.

Серверна частина знаходиться на стороні розробника. Найчастіше її роль виконує те саме програмне забезпечення, яке відповідає за генерацію і обробку контенту на сайті. Іншими словами, найчастіше серверна частина - це веб-додаток, який взаємодіє з мобільним клієнтом через інтернет за допомогою спеціального інтерфейсу (API). Сервер по праву можна вважати головною частиною: тут обробляється і зберігається інформація;

крім цього, він відповідає за синхронізацію даних між пристроями.

Сучасні версії мобільних ОС мають різноманітні вбудовані механізми захисту. Так, за замовчуванням всім встановленим програмам дозволено працювати тільки з файлами у власних домашніх каталогах, а права користувача не дозволяють редагувати будь-які системні файли. Незважаючи на це, помилки, допущені розробниками при проектуванні і написанні коду мобільних додатків, призводять до пролом у захисті і відкривають двері кіберзлочинцям.

Комплексна перевірка безпеки мобільного застосування має на увазі пошук вразливостей як в клієнтської, так і в серверній частинах; крім того, не менш важливо оцінити захищеність каналу передачі даних між ними. В даному дослідженні ми розглянемо всі ці аспекти. Також ми розповімо про загрози, які підстерігають користувачів, в тому числі про тих, які обумовлені взаємодією між клієнтської і серверної частинами мобільних додатків. З методикою дослідження та портретом учасників можна ознайомитися в кінці звіту.

Уразливості клієнтських частин:

- 60% вразливостей зосереджені в клієнтської частини
- 89% вразливостей можуть бути проексплуатувати без фізичного доступу до пристрою
- 56% вразливостей можуть експлуатуватися без адміністративних прав (jailbreak або root).

Додатки для Android з критично небезпечними уразливими зустрічаються дещо частіше, ніж програми для iOS (43% проти 38%). Однак ця різниця несуттєва, і загальний рівень захищеності клієнтських частин мобільних додатків для Android і iOS приблизно однаковий. Близько третини всіх вразливостей в клієнтських частинах мобільних додатків для обох платформ мають високий рівень ризику.

Загрози мобільних додатків

Майже всі досліджені додатки знаходяться під загрозою доступу до них хакерів. У розділі про клієнтські уразливості ми відзначали, що найпоширеніша проблема мобільних додатків - небезпечне зберігання даних. Яким чином інформація може потрапити в руки зловмисників? Найпоширеніший сценарій - це зараження пристрою шкідливим ПЗ, ймовірність якого збільшується в рази на пристроях з адміністративними привілеями (root або jailbreak). Однак шкідливе ПО може підвищувати права самостійно. Наприклад, шпигунський троян ZNIU з цією метою оперує експлойтів до нашумілої уразливості

Dirty COW (CVE-2016-5195). Потрапивши на пристрій жертви, шкідливий може запитувати дозволу на доступ до призначених для користувача даних, а отримавши дозвіл, передавати дані зловмисникам. Так, експерти TheBestVPN вивчили 81 VPN-додаток з офіційного магазину Google Play і прийшли до висновку, що багато хто з них запитують насторожуючі дозволу.

Рекомендації для користувачів

Уважно ставтеся до повідомлень від додатків про запит доступу до будь-яких функцій або даними. Не варто надавати дозвіл на доступ, якщо є сумнів в його необхідності для нормального функціонування програми

Крім того, смартфон легко втратити або він може бути вкрадений. Незважаючи на те, що за замовчуванням мобільні ОС вимагають установки пароля, це вимога можна відключити, що і роблять деякі користувачі. В цьому випадку зловмисник, який отримав фізичний доступ до пристрою, підключить його до свого комп'ютера і, використовуючи спеціальні утиліти, витягне з пам'яті пристрою чутливу інформацію. Наприклад, якщо в Android увімкнено резервне копіювання, то, використовуючи інструмент Android Debug Bridge (ADB), можна спробувати отримати дані програми з резервної копії. Якщо є привілеї root, то витягти дані можна навіть з відключеним резервуванням. На пристроях Apple з jailbreak користувачі часто залишають для SSH стандартний обліковий запис (root: alpine), що дозволяє зловмисникові скопіювати дані програми на свій комп'ютер, підключившись по SSH. Загроза має особливу актуальність у випадку з корпоративними смартфонами або планшетами, якими користуються декілька співробітників, які знають пароль від пристрою.

Література:

1. Статистика з сайту https://marketingland.com

2. Інформація про мобільні загрози https://www.ptsecurity.com

3. Вікіпедія про Мобільну Безпеку

ГОЛОВНІ ПРИНЦИПИ СВІТУ ТЕЛЕКОМУНІКАЦІЙ ТА СТАНДАРТИЗАЦІЇ

Раус Кирило Ігорович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

На сьогодні світ телекомунікацій став частиною нашого життя: передавання та приймання знаків, письмового тексту, сигналів, зображень та звуків або повідомлень будь-якого роду дротовими, радіо, оптичними або іншими електромагнітними системами зробили наше життя простішим та більш організованим. Без телекомунікацій важко уявити більшість світових організацій, адже кожна з них зацікавлена у зв'язку та повній взаємодії з клієнтом, публікації та інформування про нові послуги чи товари, створенні реклами та популяризації власного бренду через телекомунікації. Разом з тим, надзвичайно важливою роллю у сучасному світі телекомунікацій володіє стандартизація. Метою стандартизації у сфері телекомунікацій є створення єдиної системи державних і галузевих стандартів та інших нормативних документів, які визначають вимоги до телекомунікаційних мереж, їх технічних засобів та якості телекомунікаційних послуг, а також гармонізація цих вимог з вимогами міжнародних нормативних документів.

Вимоги державних і галузевих стандартів, інших нормативних документів щодо технічних засобів телекомунікацій є обов'язковими для всіх виробників і постачальників технічних засобів, науково-дослідних, проектних та будівельних організацій, а також для операторів, провайдерів телекомунікацій. Вимоги до якості послуг є обов'язковими для операторів, провайдерів телекомунікацій, що надають телекомунікаційні послуги на території України. Кожна держава повинна враховувати інтереси та безпеку своїх громадян, саме для цього створені відповідні державні органи, метою яких є максимальне задоволення попиту споживачів на телекомунікаційні послуги, створення сприятливих організаційних та економічних умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних мереж з урахуванням інтересів національної безпеки у сфері телекомунікацій.

Сучасні телекомунікації засновані на низці ключових понять, які переживали прогресивний розвиток та вдосконалення протягом більш ніж століття. Телекомунікаційні технології можуть, перш за все, бути розділені на дротові та бездротові. Однак, в цілому, основна телекомунікаційна система складається з трьох частин, які завжди присутні в тій чи іншій формі: передавач, який приймає інформацію та перетворює її в сигнал; середовище передачі, яке також називається фізичним каналом, що несе сигнал. Прикладом може бути «вільний оптичний канал»; приймач, який приймає сигнал з каналу та

перетворює його назад у доступну інформацію для одержувача. Наприклад, у радіомовленні підсилювач потужності є передавачем, радіотрансляційна антена — це інтерфейс між підсилювачем та «вільним оптичним каналом». Вільний оптичний канал є середовищем передачі. Антена приймача — це інтерфейс між вільним оптичним каналом та приймачем. Далі, радіоприймач є кінцевим пунктом радіосигналу, саме там він перетворюється з електрики в звук, для того щоб люди могли слухати його.

Телекомунікації мають значний соціальний, культурний та економічний вплив на сучасне суспільство. Кілька наступних абзаців обговорюють вплив телекомунікацій на суспільство.

У мікроекономічному масштабі компанії використовували телекомунікації для створення глобальних ділових імперій. Це повністю зрозуміло у випадку інтернет-магазинів на кшталт Amazon.com, хоча, на думку академіка Едварда Ленерта, навіть звичайна мережа роздрібних магазинів, як Wallmart, використовує кращу інфраструктуру телекомунікацій у порівнянні з її конкурентами

У макроекономічному масштабі, Ларс-Гендрік Рьоллер та Леонард Ваверман запропонували причинний зв'язок між гарною телекомунікаційною інфраструктурою та економічним зростанням.

Телекомунікації зіграли значну роль у соціальних відносинах. Тим не менш, такі пристрої, як телефони, спочатку рекламувались з акцентом на практичність (наприклад, можливість ведення бізнесу або замовлення послуг до дому) не звертаючи акцент на соціальну значущість. Лише наприкінці 1920-х і 1930-х років соціальна значущість пристрою стала основною в телефонній рекламі. Нові акції почали звертатися до емоцій споживачів, підкреслюючи важливість соціальних бесід і залишаючись пов'язаними з родиною та друзями., закриття програм чи завершення сесії користувача.

На жаль, на сьогодні перед усім світовим суспільством стоїть надзвичайно складна задача: захист телекомунікаційних мереж та стандартизація надання та отримання телекомунікаційних послуг. Усе частіше абоненти мобільного зв’язку скаржаться на списання без їх відома коштів за контент-послуги, які вони не замовляли і не споживали. За допомогою ринкових механізмів та діючих регуляторних актів проблему не може бути розв’язано, оскільки прийняття обов’язкових до виконання нормативно-правових актів, у тому числі з питань захисту прав споживачів під час надання та отримання телекомунікаційних послуг є прерогативою держави. Сьогодні

обов'язково повинні бути запроваджені вимоги до надавачів електронних довірчих послуг згідно з європейським законодавством, зокрема розробку відповідного захисту, як власних систем телекомунікацій, так і захисту відповідних даних користувача. Найбільш значну роль у стандартизації телекомунікаційних мереж відіграє сектор ITU-T що до 1993 р. іменувався як Міжнародний консультативний комітет з телефонії і телеграфії (МККТТ) (Consultative Committee on International Telegraphy and Telephony, CCITT). Основу діяльності ITU-T становить розробка міжнародних рекомендацій — стандартів у сфері телефонії, телематичних служб, передачі даних, аудіо- та відеосигналів. Свою роботу ITU-T будує на вивченні досвіду різних організацій, а також на результатах власних досліджень. Раз на чотири роки видаються праці ITU-T у вигляді так званої «Книги», що насправді являє собою цілий набір звичайних книг, згрупованих у випуски, які, у свою чергу, поєднуються в томи. Кожний том і випуск містять логічно взаємозалежні рекомендації. Основні рекомендації ITU-T постійно оновлюються на сайті організації.

Література:

1. *Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації. URL: https://spz.nkrzi.gov.ua/golovna/yakist-poslug/natsionalni-ta-mizhnarodni-standarty/*
2. *Вікіпедія.Телекомунікації.*
3. *Загальнодоступні телекомунікаційні послуги. URL : https://protocol.ua/ua/pro_telekomunikatsii_stattya_62/*
4. *Стисла характеристика організацій зі стандартизації. URL : https://www.znanius.com/3588*
5. *Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua*

ДОСЛІДЖЕННЯ ОСНОВНИХ ПИТАНЬ ТА ТРУДНОЩІВ ВПРОВАДЖЕННЯ ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ

Рєзнік Роман Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Впровадження власних центрів сертифікації ключів це якраз те завдання яке потрібно виконувати ІТ-відділам підприємств. Це все тому, що тут постає питання безпечної аутентифікації, захисту даних, що передаються та зберігаються, потреба в використанні електронного цифрового підпису та багато інше. Не всі ці задачі можуть бути вирішені постачальниками зовнішніх засобів впровадження центрів сертифікації. Завдання впровадження та підтримки власних інфраструктур є досить актуальним, тому варто розібратися з основними питаннями та труднощами їх впровадження, від законодавчих до апаратно-програмних.

Взагалі, цих питань може бути досить багато, адже для кожного підприємства потрібно розробляти свою стратегію розгортання центрів сертифікації, адже в кожної компанії свої задачі, і треба орієнтуватись саме на них. Основні нормативні акти, які регламентують використання в України електронного цифрового підпису, зокрема, Закон України «Про електронний цифровий підпис» [1] та Закон України «Про електронні документи та електронний документообіг» [2] були прийняті ще у 2003 році. Безумовно, прийняття вказаних законів мало позитивне значення і сприяло певному поширенню використання електронно-цифрового підпису.

Разом з тим, у сфері приватно-правових відносин електронний цифровий підпис не став доступною і зручною альтернативою використання паперових документів та звичайних підписів і печаток.

Такий стан речей обумовлений, не в останню чергу, складністю адміністративних процедур, дотримання яких вимагається для створення та розвитку суб'єктів інфраструктури, яка необхідна для поширення сфери використання електронних цифрових підписів.

Відповідно ст. 3 Закону України «Про електронний цифровий підпис», «Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису або печатки у разі, якщо: електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису; особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті» [1].

В цьому контексті постає питання щодо вимог до суб'єктів цих правовідносин, які мали б забезпечити можливість використання електронних цифрових підписів [3]. Це більше відноситься до комерційних центрів сертифікації. Щодо впровадження власних, постають питання з самого проектування систем, такі як: кількість рівнів ієрархії у структурі центру сертифікації; сертифікати яких саме типів потрібно використовувати; методи захисту центрів сертифікації; потреби в різних політиках видачі сертифікатів тощо.

Якщо вирішувати питання вибору схеми розгортання центру сертифікації, то вибір однорівневої схеми доречний, якщо потреби для компанії не перевищують базових наборів криптографічних сервісів, а також кількість кінцевих користувачів не велике. В такому випадку, центр сертифікації не

від'єднується від мережі, і завжди доступний для видачі користувачам сертифікатів. Але все одно не потрібно проводити розвертання центру на головному комп'ютері домену, тому що це може призвести до складних проблем інформаційної безпеки підприємства.

Щодо вибору більш захищеного та надійнішого варіанту – дворівневої схеми розгортання центру сертифікації, тут постає питання чи виводити кореневий центр з мережі та переносити на центри, що підписують, сертифікати вручну, чи все ж розгорнути додатково внутрішній вебінтерфейс для спрощеного їх підписання.

Питання з впровадження трьох- та більш рівневих схем уже відносяться до великих компанії, або компаній з потребами у високій захищеності даних. Наприклад, існує потреба з використання різних політик сертифікатів, яка обумовлена тим, що філіали компанії знаходяться в різних країнах. Або як ще варіант, який часто практикується в великих компаніях – необхідність в роздільному керуванні різними командами.

Крім того, різні вимоги законодавства на різні напрямки компанії діють порізному, наприклад для фінансової або банківської установи можуть існувати окремі, або додаткові спеціалізовані правила до криптопровайдера, довжини ключа і т.п. Отже, проблеми та труднощі впровадження центрів сертифікації чекають на кожному кроці, але найбільше залежать від напрямку діяльності підприємства та його політики.

Література:

1. Про електронний цифровий підпис [Текст] : Закон України від 22.05.2003 р. № 852-IV // Голос України. – 2003. – № 119.

2. Про захист персональних даних [Текст] : Закон України від 01.10.2010 р. № 2297-VI //Голос України. – 2010. – № 172.

3. Бойко Д. В. Вимоги до центрів сертифікації ключів / Д. В. Бойко // Право та інновації. – 2014. – № 3. – С. 43–48.

ОСОБЛИВОСТІ ПОБУДОВИ ЦЕНТРІВ СЕРТИФІКАЦІЇ КЛЮЧІВ НА ПІДПРИЄМСТВАХ

Рєзнік Роман Вікторович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Все частіше в бізнесі зустрічається впровадження електронного документообігу, віддаленої роботи персоналу, та при цьому виникає проблема довіри до ідентифікації користувачів певної інформаційної системи підприємства. Використання методів та алгоритмів асиметричної криптографії створило середовище безпечного обміну криптографічними ключами користувачів з системою, які можуть знаходитись далеко один від

одного, але проблема аутентифікації цього ключа залишається. Уникнути цієї проблеми можна за допомогою розгорнутої інфраструктури відкритих ключів, основний компонент якої – центр сертифікації ключів, що візьме на себе функцію перевірки його автентичності.

На сьогоднішній день існує три типи побудови мережі центрів: побудова по типу дерева (ієрархічна), побудова по типу мережі та комбінована схема, при якій кореневі центри дерев можуть бути об'єднані в мережу. Кожна модель має свої переваги та недоліки.

Ієрархічна модель, основана на ієрархії ЦС, що починається від єдиного кореня. Усі ЦС підпорядковані одному кореневому ЦС.

Якщо розглянути ієрархічну модель побудови центрів сертифікації, то для неї характерні наступні переваги [1]: повна підпорядкованість системи; швидкодія системи по доступу до сертифікатів; невеликий шлях сертифіката між двома центрами; невелика кількість ключів інших центрів сертифікації, якими повинен володіти центр. Серед недоліків структури такого типу можна відзначити: великий трафік з передачі ключів відразу після сертифікації; величезний об'єм бази при формуванні нового центру сертифікації у тому випадку, коли вже є достатньо розгалужена та об'ємна система центрів сертифікації та велика кількість ключів.

Друга архітектура сертифікації – мережева модель, заснована на взаємній сертифікації (крос-сертифікації) ЦС, що не підпорядковані один одному.

Що стосується моделі з мережевою структурою, то основними перевагами такої структури є [1]: можливість прямої передачі сертифікатів між центрами будь-яких рівнів; сертифікат може бути перевірений будь-яким абонентом, незалежно від його підпорядкування. Серед недоліків структури такого типу можна відзначити: необхідність виділення одного головного центру, який буде виконувати сертифікацію ключів усіх інших центрів сертифікації; необхідність усім центрам знати сертифікаційні ключі інших центрів; величезний обмін даними між центрами, які по запитам від інших центрів чи абонентів повинні видавати сертифікати.

Комбінована схема має переваги мережевої та ієрархічної систем, але збільшується навантаження на кореневі центри, які самі по собі повинні бути розподіленими системами. Тому можна сказати, що найбільш вірною для невеликих відкритих систем сертифікації є мережева модель. Якщо система сертифікації є внутрішньою, корпоративною або банківською, то можна однозначно вважати найбільш придатною до застосування систему ієрархічного типу з системою поширення

сертифікатів по адресам. Якщо створюється система PKI для групи самостійних підрозділів, тим більше для загальнодержавного масштабу, то використовується комбінована схема [2].

Отже, при виборі оптимальної ієрархії ЦС слід шукати баланс між гнучкістю і практичною доцільністю з урахуванням капітальних і операційних витрат на утримання центрів сертифікації.

Література:

1. Основні принципи побудови центрів сертифікації ключів. Центр сертифікації ключів «Джерело» та його можливості / Іван Горбенко, Олена Качко, Олександр Волощук та ін.] // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2005. – Вип. 10. – С. 143-152.

2. Лекція 18. Інфраструктура відкритих ключів, що побудована на сертифікатах [Електронний ресурс] // 2016 – Режим доступу до ресурсу: https://studfile.net/preview/5367447/.

ЩОДО НЕОБХІДНОСТІ РОЗРОБКИ МЕТОДИК ТА ГЛУБОКОГО АНАЛІЗУ ДЛЯ ЗАПОБІГАННЯ ІНСАЙДЕРСКИХ АТАК НА БАНКІВСЬКІ СТРУКТУРИ

Рогозільніков Олександр Олегович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Банківська сфера завжди була найважливішою складовою сучасного світу. Інформація якою володіє банківський сектор та її обсяг є колосальним. Однією с найважливіших частин банківського сектору завжди є захист інформації, збереження банківської таємниці та надважливої інформації. Основною ланкою розвитку банківського сектору є використання ЕПС (Електронних платіжних систем), саме вони відповідають за дуже великий обсяг інформації який передається банківськими системами та каналами. Ці системи захищенні використанням SSL сертифікату, вони проходять тестування PSI DSS та використовують технологію 3D-Secure для додаткової ідентифікації користувачів. Та чи є атаки на ці системи одним із найголовніших питань захисту інформації?

Завжди існує найголовніша загроза будь-якій інформації в незалежності від систем які використовуються - це інсайдерські атаки. Їх суть закладається в найважчому в чому можливо розібратися та запобігти втраті даних – людський мозок та його поведінка. Інсайдереми можуть бути як люди які самі можуть бути джерелом небезпеки або вони можуть представляти собою зброю в руках більш крупних конкурентів, терористичних

організацій тощо. Таким чином людина яка є інсайдером може здійснити ряд критичних правопорушень. Шахрайство та використання соціальної інженерії з подальшим проникненням також вважається інсайдерською атакою яка може спричинити втрату критичної інформації, розголошення банківської таємниці.

Задача аналізу повинна вирішуватись за допомогою правоохоронних органів та використанням штучного інтелекту та машинного навчання задля ідентифікації можливості інсайдерської атаки. Потрібно створити підрозділ який буде включати в себе спеціалістів в області штучного інтелекту та підрядних правоохоронців. Це можуть бути статисти, експерти в області людської поведінки. Також одним із важливих рішень для покращення та прискорення розробки потрібних методик та покращення аналізу потрібно впровадити перевірку кадрів на поліграфі задля звітності яка піде в обробку для створення методик захисту від шахрайства та інсайдерських атак штучним інтелектом та моделями машинного навчання.

Література:

1. НЕЙРОМЕРЕЖЕВА ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ НА ОСНОВІ АНАЛІЗУ ЖУРНАЛІВ АКТИВНОСТІ , КОРИСТУВАЧІВ, ISSN2409-7292 [Електронний ресурс] / В.А. Савченко, В.В. Савченко, С.В. Довбешко, М.М. Алексєєв, А.М. Зідан, - 2018. – Режим доступу до ресурсу : http://dspace.tneu.edu.ua/bitstream/316497/1537/1/10_%D1%84%D0%B0%D1%85.pdf

2. ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ ОНТОЛОГІЇ ДЛЯ ПРОЕКТУВАННЯ ТА АНАЛІЗУ КСЗІ [Електронний ресурс] / Олександр Архипов, Олег Козленко – 2017. – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/325942555.pdf

ХАРАКТЕРНІ УРАЗЛИВОСТІ СИСТЕМ "РОЗУМНОГО БУДИНКУ" ПОБУДОВАНИХ НА ОСНОВІ KNX-CRESTRON ТЕХНОЛОГІЙ ТА ЗАСОБИ ПРОТИДІЇ

Семенова Інна Дмитрівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Інтернет речей (IP) - один з найперспективніших напрямків розвитку інформаційних технологій на сьогодні. Частиною IP є концепція "Розумний будинок", яка дозволяє інтегрувати набір самостійних технологій, таких як керування світлом, кліматом, охоронною системою, тощо, в єдиний диспетчерський пункт керування будівлею. Для цього використовуються технології різного рівня, від польової шини, що реалізую фізичну комутацію до технологій вищого рівня, які базуються на мережевій взаємодії.

З боку захисту інформації, варто приділити увагу недолікам безпосередньо технологій інтеграції та мережевими уразливостями. Не можливо відмежувати їх один від одного, оскільки вони нероздільно взаємопов'язані протоколами взаємодії. Варто розглядати технічні канали витоку інформації, оскільки неможна недооцінювати фізичну складову системи.

1. Шифрування

Однією з найбільш поширених проблем системи розумного будинку є слабке або, навіть, відсутнє шифрування.

Деякі системи взагалі не мають можливості шифрування, наприклад, передача сигналів шиною KNX – усі сигнали передаються в незашифрованому вигляді, як двійкові послідовності, сигнальним кабелем, в даному випадку ми не маємо технічної можливості використати додаткове обладнання для апаратного або програмного шифрування, оскільки це, по-перше, значно підвищить вартість системи, а, по-друге, сповільнить її до неприйнятного рівня.

В даному випадку єдиним рішенням буде підвищення рівня фізичної безпеки та виключення можливості доступу зловмисника до фізичного обладнання (шина, пристрої керування та керовані пристрої). Оскільки шина розташована локально та не має доступу до мережі, фізичного периметру захисту буде достатньо для зниження ризику до прийнятного рівня.

Інші технології, наприклад система керування вищого рівня побудована на обладнанні Crestron, мають вбудовані можливості шифрування.

2. Віддалене підключення

Як правило, використовується VPN-підключення зі стандартнім налаштуванням, або «перенаправлення портів», знову ж таки, зі стандартними відкритими портами. Подібне нехтування може призвести до того, що, хто завгодно зможе підключитися до керування системою.

Розглянемо деякі шляхи зниження ризику.

2.1 VPN-підключення

Існує декілька видів VPN: Найбільш поширені — PPTP VPN, Site-to-Site VPN, L2TP VPN, IPsec, SSL, MPLS VPN та Hybrid VPN.

PPTP VPN - це протокол тунелювання точка-точка. Як видно з назви, PPTP VPN створює тунель і захоплює дані. Це найпоширеніший тип VPN. PPTP VPN дозволяють підключитися до мережі VPN через існуюче інтернет-підключення. Цей тип VPN прекрасно підходить як для бізнесу, так і для домашнього використання. Для доступу до мережі використовується пароль. PPTP ідеальні для дому та бізнесу, так як вони не вимагають установки додаткового обладнання і дозволяють обходитися дешевими і нескладними додатками. PPTP добре сумісні з Windows, Mac і Linux.

І хоча PPTP VPN демонструють безліч переваг, не обійшлося без недоліків. Головний з них - це те, що протокол PPTP не використовує шифрування. Крім того, основа PPTP - це протокол PPP, що також не забезпечує високий рівень безпеки.

Site-to-Site VPN - Вузол-вузол або Роутер-Роутер - це найпоширеніший тип VPN в бізнесі. Особливо це характерно для компаній з офісами як в різних частинах однієї країни, так і в декількох країнах, що дозволяє зв'язати всі комп'ютери в єдину мережу. Також вони відомі як інтранет-VPN (VPN по внутрішній мережі). Інший варіант також можливий. Компанії, що використовують VPN вузол-вузол, підключаються до серверів інших компаній таким же чином, як і екстранет-VPN. Говорячи простою мовою, цей тип VPN - свого роду міст, що з'єднує мережі в різних локаціях, забезпечуючи безпечне з'єднання і підключення до інтернету.

Як і PPTP, VPN типу вузол-вузол створює безпечну мережу. Однак, виділена лінія не передбачена, так що різні комп'ютери компанії можуть підключатися до мережі. На відміну від PPTP, шифрування проводиться або за допомогою спеціальних пристроїв, або за допомогою додатків на обох кінцях мережі.

L2TP VPN. L2TP означає «Протокол тунелювання другого рівня», він був розроблений компаніями Microsoft і Cisco. VPN на основі протоколу L2TP поєднується з іншим протоколом, що забезпечує більш безпечне з'єднання. При протоколі L2TP формується тунель між двома точками підключення L2TP, а також за допомогою іншого протоколу, наприклад IPsec, проводиться шифрування даних.

L2TP діє подібно PPTP. Головне подібність - відсутність шифрування і основа на протоколі PPP. Різниця ж - це захист і збереження даних. VPN на основі L2TP забезпечують більш безпечне і надійне з'єднання. В першу чергу за рахунок додаткового «паролю» - спільного ключа, необхідного для підключення. Тобто кожен користувач має знати не лише власні логін та пароль, а й спільний ключ, для підключення.

IPsec - це скорочення, що означає «Безпека інтернет-протоколу». IPsec - це VPN-протокол, який використовується для того, щоб забезпечити безпеку в мережі. Протокол встановлює тунель до віддаленого вузла. Кожна сесія перевіряється, пакети даних шифруються, так що протокол IPsec забезпечує високий рівень безпеки з'єднання. Існує два режими, в яких працює цей протокол. Транспортний і тунельний. Обидва служать для захисту передачі даних між різними мережами. У транспортному режимі шифрується повідомлення в пакеті

даних. У тунельному режимі шифрується весь пакет даних. Перевага використання IPsec полягає в тому, що він може бути застосований на додаток до інших протоколах, щоб підвищити захист мережі.

І хоча IPsec - це корисний і зручний протокол, однак основний мінус - це довгий час встановлення клієнтських додатків.

SSL and TLS. SSL - це протокол захищених сокетів, TLS - безпека на транспортному рівні. Вони працюють як один протокол. Обидва використовуються для створення VPN. У цьому підключенні веб-браузер працює як клієнт, користувач отримує доступ до спеціальних додатків замість всієї мережі. SSL і TSL використовуються в онлайн-продажах. SSL і TSL надають захищену сесію від браузера до сервера з додатком. Браузер легко перемикається на SSL, не вимагаючи ніяких додаткових дій з боку користувача. Абсолютна більшість сучасних браузерів вже включає в себе SSL і TSL. SSL-підключення містить https замість http в адресі.

MPLS VPN. VPN-сервіси з підтримкою технології багатопротокольной комутації з використанням міток (MPLS) найкраще використовувати для підключень типу сайт-к-сайту. Все тому, що MPLS - це найбільш гнучкий варіант з максимум можливостей для адаптації. MPLS ґрунтуються на певних стандартах, які використовуються для прискорення розподілу мережевих пакетів по безлічі протоколів. VPN-сервіси з підтримкою MPLS - це системи, що представляють собою VPN-сервіси, налаштовані для роботи з інтернет-провайдерами, коли два або більше сайтів можуть об'єднатися між собою, формуючи VPN, використовуючи для цього потужності одного і того ж інтернет-провайдера. Втім, найбільшим мінусом VPN-сервісів з підтримкою MPLS є той факт, що таку мережу налаштувати куди складніше, ніж інші VPN. Складніше і вносити в неї модифікації. Як наслідок, послуги VPN-сервісів з підтримкою MPLS обходяться користувачам дорожче.

Hybrid VPN. Гібридна мережа VPN поєднує в собі MPLS і IPSec. Обидва типи використовуються окремо на різних вузлах. Однак, іноді вузол допускає одночасне підключення обох типів протоколів. Це робиться з метою підвищити надійність MPLS за допомогою IPSec.

IPSec, як уже згадувалося раніше, вимагають наявності певного обладнання. Зазвичай це роутер або багатоцільове пристрій безпеки. За його допомогою дані шифруються і утворюють VPN-тунель. MPLS використовуються на каналі передачі інформації за допомогою передавального обладнання.

Для з'єднання цих двох типів VPN встановлюється шлюз, де усувається IPSec і проводиться підключення до MPLS зі збереженням безпеки даних.

Гібридні VPN використовуються компаніями, так як MPLS дуже часто не підходить для їх вузлів. MPLS забезпечує безліч переваг в порівнянні із загальним підключенням, однак ціна висока. За допомогою гібридної мережі ви можете підключитися до центрального вузла через віддалений. Гібридні VPN найбільш дорогі, але при цьому дуже гнучкі в налаштуванні[1].

Найчастіше використовуються L2TP підключення оскільки це баланс достатньої захищеності та прийнятної вартості, але завжди варто пам’ятати про особливості встановлення паролів, а саме притримуватися таких правил:

1. Пароль має бути не менш ніж 8 символів
2. Необхідно розширити алфавіт символів паролю, це робиться за рахунок використання літер різного регістру, цифр, спеціальних символів
3. Пароль має знати лише власник системи
4. Пароль необхідно змінювати не рідше ніж кожні 6 місяців та якнайшвидше у разі компрометації, підозри компрометації, паролю[2].

Перші три правила стосуються і спільного ключа.

Розглянемо на прикладі необхідність дотримання цих правил.

Час повного перебору всх можливих паролів заданого алфавіту при швидкості перебору 10,000,000 паролів/сек				
Алфавіт, символів	Довжина паролю, символів			
	6	8	10	12
26 (латиниця одного регістру)	31 с.	5 год. 50 хв.	163,5 доб	303 р.
52 (латиниця, змішаний регістр)	33 хв.	62 доби	458 р.	1239463 р.
62 (латиниця різного регістру та цифри)	95 хв.	252 доби 17 год.	2661 р.	10230425 р.
68 (латиниця різного регістру, розділові знаки та цифри)	2 год. 45 хв.	529 діб	6703 р.	30995621 р.
80 (латиниця різного регістру, розділові знаки, спецальні символи та цифри)	7 год. 30 хв.	5 р. 4 міс.	34048 р.	217908031 р.

Рис. 1 – Залежність часу підбору паролю від довжини алфавіту та кількості символів

Також, часто використовується SSL-підключення, це гарне рішення з точки зору безпеки, але часто у інтеграторів

виникають проблемі на етапі отримання сертифікатів, що сповільнює введення системи в експлуатацію та призводить до відмови від будь-якого захисту з боку замовника для пришвидшення робот.

В такому випадку краще зупинитися на, умовно, слабшому захисті, задля забезпечення прийнятного рівня ризику.

2.1 Переправлення портів

Переадресація портів або зіставлення портів - це додаток перетворення мережевих адрес, яке перенаправляє запит на обмін даними від однієї комбінації адреси і номера порту до іншої, коли пакети проходять через мережевий шлюз, такий як маршрутизатор або міжмережевий екран.

Цей метод використовується коли з якихось причин, замовник не згоден використовувати VPN-підключення, частіше через недостатню обізнаність в питаннях безпеки.

Зрозуміло, що такий метод не забезпечує достатньо рівня захищеності, але, якщо він використовується, необхідно, щонайменше, використовувати не стандарті порти для переправлення.

3. Підміна DHCP сервера

Підміна DHCP сервера, яка дозволяє зловмиснику змусити клієнта використовувати нелегітимний вузол в якості шлюза за замовчуванням, виключити таку можливість для зловмисника дозволяє коректне налаштування мережі:

- Увімкнути dhcp snooping
- Визначити довірені порти
- Вказати адресу довіреного DHCP сервера який доступний через довірений порт.

4. Маскування під легітимною MAC адресою

Зловмисник знаходиться в мережі з параметрами дозволеного пристрою, це дозволяє перехоплювати певну інформацію, або «підставити» пристрій – власник буде вважати, що це його пристрій «збожеволів» та атакує мережу. Найпростіше рішення – гарантована авторизація пристроїв у мережі після кожного перепідключення[3].

Ідентифікація (від латинського identifico - ототожнювати): присвоєння суб'єктам і об'єктам ідентифікатора і / або порівняння ідентифікатора з переліком привласнених ідентифікаторів.

Автентифікація (від грецького: αυθεντικός; реальний або справжній): підтвердження достовірності чого-небудь або кого

небудь. Наприклад, введений пароль - це підтвердження автентичності заявленого логіна.

Авторизація є функцією визначення прав доступу до ресурсів і управління цим доступом. Авторизація - це не те ж саме що ідентифікація та автентифікація: ідентифікація - це називання особою себе системі; автентифікація - це встановлення відповідності особи, призначеному ним самим ідентифікатором; а авторизація - надання цій особі можливостей у відповідність до покладених йому правами або перевірка наявності прав при спробі виконати будь-яку дію[4].

Access Control List або ACL - список управління доступом, який визначає, хто або що може отримувати доступ до об'єкта (програми, процесу чи файлу), і які саме операції дозволено або заборонено виконувати суб'єкту. Використання таких списків достатньо простий та ефективний метод захисту від підключення нелегітимних пристроїв та користувачів

5. Порушення електропостачання

Нажаль, дуже часто, власники або інтегратори нехтують необхідністю встановлення пристрою гарантованого електропостачання, або генератора. Перебої можуть призвести до виходу зі строю елементів системи, порушенню роботи програми автоматизації, відключенню або порушенням в роботі ППК – усе це може призвести до нелегітимного доступу, як до інформації, що циркулює в системі, так и безпосередньо до об’єкту.

Проблема вирішується встановленням пристрою гарантованого живлення або додаткового незалежного джерела електропостачання.

6. Витік інформації акустичними каналами

Одним із різновидів датчиків охоронної сигналізації є датчики розбиття віконного скла та вібраційні датчики, котрі в якості чутливого елементу використовують високочутливі мікрофони та п’єзоелементи, відповідно, і реагують на події в діапазоні звукових хвиль. Ці датчики з’єднані з пультом охорони багатопровідним шлейфом, з допомогою якого здійснюється живлення датчиків постійною напругою, а від нього до пульта охорони передаються логічні сигнали про стан, в якому знаходиться датчик та цілісність самого датчика.

Відомо, що пульти охорони, як правило, знаходяться за межами контрольованої зони і можуть бути віддалені від датчиків на відстань до 100 і більше метрів. В силу акустоелектричного перетворення, в таких охоронних датчиках на струмопровідному шлейфі останніх, можуть утворюватися небезпечні напруги в звуковому діапазоні частот, які можуть

бути використані зловмисником для нелегального прослуховування приміщень при несанкціонованому підключенні до шлейфу[2]. В ході досліджень було доведено, що до 90% тексу може бути розшифровано за допомогою аналізу характеристик цих напруг.

Література:

1. https://ru.vpnmentor.com/

2. Бржевський М.В., Пузняк З.М. Дослідження процесу акустоелектричного перетворення в охоронних датчиках. - Сучасний захист інформації №2(34), 2018 ст.65-71

3. Ярочкин В.И., Информационная безопасность. Учебник для студентов. 2-е изд. - М.: Академический Проект, Гаудеамус, 2004. – 544 ст.

4. https://wiki.diphost.ru/Authentication

ДОСЛІДЖЕННЯ ШЛЯХІВ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Смолєв Євген Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Ransomware є типом зловмисного програмного забезпечення, яке при відкритті блокує систему та шифрує пристрій, щоб ніхто більше не міг ним користуватися. Ransomware – одна з найскладніших та руйнівних загроз. Комп'ютер або сервер, які постраждали, залишатимуться заблокованими, поки від імені компанії не буде виплачено великий викуп, хоча деякі хакери схильні не виконувати розблокування, яке вони обіцяють, внаслідок чого бізнес ще більше страждає. За даними IBM X-Force використання зловмисного програмного забезпечення суб'єктами загроз продовжує коливатися, оскільки ransomware, криптовалютні майнери та ботнети лідирували у різних точках у 2019 році. Очікується, що ця тенденція продовжиться і в 2020 році, тобто організаціям потрібно буде захистити себе від різноманітних загроз, які змінюються з часом та навчитися їх виявляти.

Національний інститут стандартів і технологій США (NIST) визначає вразливість, як «слабкість в інформаційній системі, процедурах безпеки системи, внутрішньому контролі чи впровадженні, які можуть бути використані джерелом загрози». Таким чином, вразливість – це слабкість, яку можуть використовувати противники для досягнення зловмисної цілі. Традиційно фахівців з кібербезпеки навчають розглядати вразливості з технічної точки зору, наприклад, недоліки, виявлені в програмних платформах, або проблеми з

конфігурацією, якими можуть скористатися хакери для отримання доступу.

Необхідно також відзначити, що вектори атак на корпоративні інфраструктури ґрунтуються на експлуатації поширених вразливостей та недоліків, для усунення яких, як правило, досить застосувати базові принципи забезпечення інформаційної безпеки: використовувати сувору парольну політику; захищати привілейовані облікові записи; не зберігати конфіденційну інформацію у відкритому вигляді або у відкритому доступі; обмежити число доступних для підключення на мережевому периметрі інтерфейсів мережевих служб; захищати або відключати в локальній обчислювальній мережі протоколи канального або мережевого рівня, які не використовуються, та розділяти мережу на сегменти; мінімізувати привілеї користувачів і служб; регулярно оновлювати програмне забезпечення і встановлювати оновлення безпеки операційної безпеки; для своєчасного виявлення атак використовувати SIEM-системи; для захисту веб-додатків використовувати фаєрвол веб-додатків; проводити регулярні тренінги, спрямовані на підвищення обізнаності користувачів в питаннях інформаційної безпеки; -для захисту від поширення шкідливого програмного забезпечення із застосуванням соціальної інженерії використовувати спеціалізовані антивірусні рішення; -регулярно проводити тестування на проникнення для своєчасного виявлення нових векторів атак і перевірки вжитих заходів захисту на практиці [2].

Через збільшення кількості загроз кібербезпеки, з якими стикаються організації, спостерігається відповідне зростання кількості інструментів сканування вразливостей. Існує безліч безкоштовних та преміальних інструментів для організацій на вибір. Два сканери, що найчастіше використовуються для виявлення вразливостей– це Nessus та Nmap (останній з яких може бути використаний, як основний інструмент для виявлення вразливостей через його функцію сценаріїв). Nmap відрізняється високою гнучкістю і може бути налаштований на задоволення конкретних потреб користувачів у скануванні. Він швидко відображає нову мережу та надає інформацію про пов’язані з нею активи та їхні вразливості. Nessus можна розглядати як просунуту версію сканера Nmap. Це пояснюється тим, що Nessus може виконувати поглиблену оцінку вразливостей хостів, підключених до мережі [3].

Таким чином, грамотно використовуючи сканер безпеки мережі, можна значно посилити захист інформаційної системи. Сканер автоматизує аудит безпеки, сканує мережу і веб-сайти на

предмет різних вразливостей. Також сканер може генерувати список пріоритетів за ризиками, які потрібно усунути, описувати уразливості і надавати список заходів щодо їх усунення.

Література:

1.IBMX-ForceThreatIntelligenceIndex[Електронний ресурс]–Режим доступудо ресурсу: https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf (дата звернення: 17.10.2020).

2. Актуальні кіберзагрози: ІІІ квартал 2017 року [Електронний ресурс] –Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics (дата звернення: 17.10.2020).

3. VulnerabilitiesandvulnerabilityScanning. [Електронний ресурс] – Режим доступу до ресурсу: https://www.sans.org/reading-room/whitepapers/basics/paper/421 (дата звернення: 17.10.2020).

МЕТОДИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА НА БАЗІ ПЛАТФОРМИ 1С:ПІДПРИЄМСТВО 8.

Сокол Антон Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Необхідність успішного функціонування в умовах жорсткої конкурентної середовища диктує свої вимоги до ефективності бізнес-процесів підприємства. Рішення завдання підвищення ефективності нерозривно пов'язане із забезпеченням інформаційної підтримки процесів, тому сьогодні практично ні у кого не викликає сумніву необхідність побудови інформаційної системи підприємства. Більшість людей, які приймають рішення в цій галузі, поділяють думку, що питання побудови інформаційної системи слід вирішувати в контексті завдань вдосконалення бізнес-процесів.

Розвиток різних сфер людської діяльності на сучасному етапі неможливе без широкого застосування обчислювальної техніки та створення інформаційних систем різного спрямування. Обробка інформації в подібних системах стала самостійним науково-технічним напрямком. Після етапу побудови інформаційної моделі починається проектування системи. На цьому етапі проводиться вибір технологічних рішень, на основі яких буде побудована інформаційна система.

Інформація в сучасному світі перетворилася в один з найбільш важливих ресурсів, а інформаційні системи стали необхідним інструментом практично у всіх сферах діяльності. Інформаційні системи управління підприємством надають точну, своєчасну, актуальну і повну інформацію, необхідну для полегшення, сприяння прийняттю рішень в підприємстві. Вони допомагають в ефективному і продуктивному здійсненні функцій підприємства, в плануванні і контролі. В реальних умовах

проектування - це пошук способу, який задовольняє вимогам функціональності системи засобами наявних технологій з урахуванням заданих обмежень. Різноманітність завдань, що вирішуються за допомогою інформаційних систем, привело до появи безлічі різнотипних систем, що відрізняються принципами побудови і закладеними в них правилами обробки інформації.

Аутентифікація - це основа безпеки будь-якої системи, яка полягає в перевірці достовірності даних про користувача. Система 1С:Підприємство 8 підтримує кілька видів автентифікації, які можуть використовуватися в залежності від конкретних завдань, що стоять перед адміністратором інформаційної бази:

Автентифікація OpenID Connect - це один з видів автентифікації, підтримуваних механізмом автентифікації 1С: Підприємства. OpenID Connect дозволяє системі 1С: Підприємство перевірити особу користувача на основі автентифікації, виконаної стороннім провайдером. В результаті, для того, щоб отримати доступ до прикладному рішенню 1С: Підприємства, користувачі можуть використовувати свої облікові дані на інших сайтах, що підтримують OpenID Connect автентифікацію Автентифікація OpenID Connect може бути застосована при використанні тонкого клієнта і веб-клієнта. Починаючи з версії 8.3.16 автентифікацію OpenID Connect можна використовувати і в мобільному клієнті.

OpenID-автентифікація - в цьому випадку автентифікацію користувача виконує не конкретна інформаційна база, до якої намагається підключитися користувач, а зовнішній OpenID-провайдер, який зберігає список користувачів. Перевага цього виду автентифікації проявляється тоді, коли користувач працює з великою кількістю різних інформаційних баз. Якщо використовується автентифікація 1С: Підприємства, то кожен раз, при підключенні до інформаційної бази, користувач буде повинен вводити логін і пароль. Якщо ж використовується OpenID-автентифікація, то одного разу виконавши процедуру автентифікації при підключенні до однієї з баз, в усі інші бази користувач буде заходити без запиту логіна і пароля. OpenID-провайдер буде автоматично автентифікувати користувача на основі наявної у нього інформації.

Автентифікація 1С: Підприємства - при використанні цього виду автентифікації засобами 1С: Підприємства в конфігураторі для користувача задається пароль. В результаті користувач, при початку роботи з прикладним рішенням,

повинен вибрати (або ввести) ім'я користувача і відповідний цьому імені пароль. Якщо пароль, введений користувачем, не відповідає тому, який «зберігається» в інформаційній базі, доступ до прикладному рішенню буде закритий.

Автентифікація операційної системи - у разі автентифікації засобами операційної системи в конфігураторі для користувача вибирається один з користувачів операційної системи. При виконанні автентифікації засобами операційної системи, від користувача не потрібно будь-яких дій щодо введення логіна і пароля. Система аналізує, від імені якого користувача операційної системи виконується підключення до прикладному рішенню, і на підставі цього визначає відповідного користувача 1С: Підприємство 8. При цьому діалог автентифікації 1С: Підприємства не відображається, якщо не вказано спеціальний параметр командного рядка. Якщо для користувача не вказано ні один з видів автентифікації, - такому користувачеві доступ до прикладному рішенню закритий.

Література:

1. Механизмы аутентификации 1С:Предприятие 8 [Електронний ресурс] Режим доступу: https://v8.1c.ru/platforma/mehanizmy-autentifikacii/

ПРОЕКТУВАННЯ СИСТЕМИ ЗБОРУ І КОРЕЛЯЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Стародубець Владислав Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Актуальність і своєчасність звернення до даного питання обумовлена тим, що, з безперервним розвитком інформаційних технологій та покращенням рівня життя та комфортності, комп'ютерні системи були інтегровані майже у всі аспекти людського життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається.

Системи інформаційної безпеки модернізуються і вдосконалюються практично щодня. Це все не просто так, адже постійно у світі виникають сотні та тисячі нових загроз, до яких потрібно пристосуватися, щоб забезпечити максимально ефективний захист від несанкціонованого доступу. Однак, як показує практика, просто впровадити систему безпеки мало. Наскільки б потужною, надійною і сучасною вона не була все одно необхідно запобігати виникаючим загрозам. Тобто потрібно якомога швидше реагувати на події, що надходять від системи захисту даних.

Особливо це стосується великих компаній. Найчастіше саме в подібних організаціях буває найбільше різної інформації, яку потрібно в обов'язковому порядку ретельно захищати. Але найчастіше в таких компаніях інфраструктура виявляється настільки великою і складною, що якісно реагувати на величезний потік подій ІБ буває надзвичайно складно, а іноді навіть неможливо. Саме в таких випадках приходять так звані системи збору та кореляції подій ІБ (SIEM).

За твердженням Gartner, SIEM-система повинна збирати, аналізувати і представляти інформацію з мережевих пристроїв і пристроїв безпеки. Також в цю систему повинні входити додатки для управління ідентифікацією і доступом, інструменти управління вразливостями, бази даних і додатки.

Таким чином, на основі вивчення та аналізу відповідних джерел визначимо основні особливості SIEM-систем, дослідимо та вивчимо ринок SIEM і порівняємо їх за якісними показниками також спроектуємо мережу, в яку в наслідок буде впроваджена SIEM-система і впровадимо систему.

Література:

1. Дмитрий Хамакев «SIEM: ответы на часто задаваемые вопросы»– Електронний ресурс – Режим доступу: https://habrahabr.ru/post/172389/

2. Максим Гарусев. «Системы корреляции событий: революция или эволюция?» Електронний ресурс – Режим доступу: http://www.setevoi.ru/cgi-bin/text.pl/magazines/2003/7/30

3. Олеся Шелестова «Что такое SIEM?» Електронний ресурс – Режим доступу: http://www.securitylab.ru/analytics/430777.php

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. СОЦІАЛЬНА ІНЖЕНЕРІЯ

Сябро Валерія Борисівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Що ми розуміємо під кібербезпекою? Кібербезпека – це методи, процеси та технології, що призначені для захисту програм, мереж та головне, наших даних. Дані – це актив. В сучасному світі найбільшу цінність та значимість несе інформація, а самим слабким місцем у її захисті є ж самі люди. Будь-яка організація (державні або комерційні структури , фінанси або медицина) накопичують, зберігають, оперують великою кількістю даних користувачів, клієнтів, співробітників тощо. Кожна система, що взаємодіє з ЕОМ та її безпека відіграють важливу роль у житті як компанії, так і в житті людства в цілому. Ключові слова: соціальна інженерія, фішинг, кібербезпека, конфіденційні дані.

Основна складність для суспільства і держави щодо кіберзлочинів пов'язана з тим, що сфера кіберзлочинів обросла стереотипами та міфами. Неправомірні доступи до комп'ютерної

інформації, «зломи» сайтів і поштових ящиків, атаки на ресурси та інші кіберзлочини пов'язують з складними і геніальними технічними процесами, осягнути які може далеко не кожен. Проте більшість найвідоміших кіберзлочинів просто у виконанні і цілком піддається аналізу будь-яким освіченою людиною.

Згідно з опитуванням, проведеним Zogby Analytics для Національного альянсу з кібербезпеки США в 2019 році, все більше компаній усвідомлюють, що вони є цілями кіберзлочинців. Але Маркус Ранум якось сказав: «Коли справа доходить до безпеки, то потрібно, щоб спершу хлопець, який стоїть поряд з вами, отримав кулю в голову, ніж керівництво зверне увагу на безпеку». Дуже часто керівництво, не бажає виділяти кошти на засоби запобігання витоку інформації, чи просто її захисту, в силу того, що не бачать загроз, але коли наступає той самий критичний момент, вимагає швидкого реагування та дій. Одним з таких недооцінених видів загроз є соціальна інженерія, серед яких є добре відомий всім вид спаму - фішинг. Соціальну інженерію, у сукупності з технічними знаннями систем інформаційної безпеки, використовують для досягнення наступних цілей:

1. Збір інформації про потенційну жертву.

2. Отримання конфіденційної інформації (для досягнення даної мети при тривалому спілкуванні з жертвою, соціальний інженер входить у довіру і під зручними приводами отримує необхідну інформацію).

3. Отримання інформації, необхідної для несанкціонованого доступу (НСД) [1, с. 99].

4 Змушення об’єкта здійснити необхідні соціальному інженеру дії

За оцінками Центру прийому скарг на шахрайство в Інтернеті (IC3) при ФБР, тільки в 2018 році в результаті кібератак американські компанії втратили більше 2,7 мільярдів доларів, в тому числі 1,2 мільярда доларів в результаті атак з використанням компрометації ділового листування (BEC) / компрометації електронних листів (EAC) (див. Рис.1), які дозволяли несанкціоновано переказувати кошти [2].

Рис. 1 – Втрат американських компаній з використанням компрометації

Фішинг (англ. *phishing* від *fishing* — рибальство) [3, с. 10]. Зловмисник намагається виманити в одержувача листа номер його кредитних карток чи паролі доступу до електронних платіжних систем тощо. Такий лист, зазвичай, маскується під офіційне повідомлення від адміністрації компанії. У ньому говориться, що одержувач повинен підтвердити відомості про себе і наводиться адреса сайту, який належить спамерам, із формою, яку треба заповнити. Серед даних, що потрібно повідомити, є й ті, котрі потрібні шахраям.

Типовими жертвами зловмисників є люди які не знають цінності інформації, ті які мають особливі привілеї, бухгалтерія, відділ кадрів, певні особливі відділи тощо.

Основні попереджуючі знаки соціальної інженерії [4, с. 405]:

1. Незвичайне прохання
2. Затвердження, що той хто дзвонить – керівництво
3. Новий колега, що просить про допомогу
3. Дивна адреса відправника
4. Запит на конфіденційні данні
5. Терміновість
6. Погроза у вигляді створення негативних наслідків у випадку не виконання

Щоб захистити компанії від шахрайства, необхідно навчити персонал розпізнавати соціальну інженерію та реагувати на неї, забороняти співробітникам ділитися паролями або мати загальне ключове слово, забезпечувати захист конфіденційної інформації клієнта та співробітника та впроваджувати спеціальні процедури підтвердження для тих, хто подає доступ до будь-яких даних. Параметри проти фішингу з’явились у браузерах, попереджаючи відвідувачів сайту про ненадійні або небезпечні ресурси. Фільтрація спаму може допомогти захистити від загроз, що надсилаються електронною поштою. Більш складні методи авторизації також зменшать ризик.

Література:

1. Прокоф'єв І.В. Введення в теоретичні основи комп'ютерної безпеки: навчальний посібник / І.В. Прокоф'єв - М .: МІФІ, 2008. - 287 с.

2. Звіт ФБР // Business email compromise the $26 billion scam // вересень 10, 2019. URL: https://www.ic3.gov/media/2019/190910.aspx

3. Д. Акерлоф, Р. Шиллер. Фішинг : Хто і як маніпулює вашим вибором / пер. з англ. О. Герасимчук. – К. : Наш формат, 2017. – 272 с.

4. Митник К.Д. Мистецтво обману: метод. посібник / К.Д. Митник - NYC: Wiley Books. 2008 - 273 с.

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ВИКОРИСТАННЯ СИСТЕМ DLP

Тищенко Віталій Сергійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Швидкий процес інформатизації суспільства супроводжується зростаючим ризиком втручання в роботу інформаційних систем у вигляді несанкціонованого доступу до інформації. У зв'язку з цим актуальність постійного вдосконалення систем інформаційної безпеки, використання комплексного підходу, що поєднує законодавчі, організаційні та програмні заходи. Розвиток ринкових відносин в Україні сприяв тому, що не лише державні підприємства та установи, а й об'єкти інших форм стикаються з необхідністю зберігати комерційну, технологічну та фінансову таємницю компаній, особисті дані фізичних осіб.

Інформаційні ресурси держави або суспільства в цілому, а також окремі організації та окремі особи представляють певну цінність, мають відповідний матеріальний вираз і потребують захисту від різних властивих їм впливів, які можуть зменшити цінність інформаційних ресурсів. В ринкових умовах головним рушієм прогресу є конкуренція, яка має на меті створити умови для збільшення прибутку, тому інформація за певних обставин стає об'єктом дії конкурентів [1].

Сьогодні існують досить потужні системи несанкціонованого збору інформації, високоефективні технічні засоби та добре навчені фахівці. Уникнути всіх інцидентів інформаційної безпеки неможливо, оскільки завжди можуть бути події, що спричиняють потенційну загрозу. Інцидент інформаційної безпеки - одна або низка небажаних або несподіваних подій в системі інформаційної безпеки, які можуть скомпрометувати ділові операції та поставити під загрозу захист інформації [2].

Великі організації щодня реєструють велику кількість подій, які не є інцидентами, але один пропущений інцидент

може коштувати організації дуже великих втрат аж до припинення її діяльності. Існує багато способів подолання інцидентів як на рівні організаційних процедур, так і на рівні програмних рішень.

Одним з найбільш ефективних методів є впровадження систем захисту від витоку конфіденційних даних (DLP, Data Leak Prevention). Технологія DLP надає можливість блокувати передачу конфіденційної інформації за різними каналами, а також надає інструмент для моніторингу повсякденної роботи співробітників, який дозволяє знаходити вразливі місця безпеки до інциденту [3].

Тому важливо проаналізувати захист від витоку конфіденційних даних DLP-систем. Таким чином, на основі вивчення та аналізу відповідних джерел визначимо основні особливості DLP-систем, дослідимо та вивчимо ринок і порівняємо їх за якісними показниками також спроектуємо мережу, в яку в наслідок буде впроваджена DLP-система.

Література:

1. В.В. Домарев, Д.В. Домарев. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k), Донецьк: Велстар, 2012. – 146 с.

2. Міжнародний стандарт ISO/IEC 27001 «Інформаційні технології – Методи безпеки – Системи управління інформаційною безпекою – Вимоги».

3. Johansen G. Digital forensics and incident response: an intelligent way to respond to attacks. – 2017.

КРИПТОВАЛЮТА

Туча Іван Олександрович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

За свою історію людина винайшла безліч способів вимірювати вартість речей або послуг. Мушлі і перлини, золото і банкноти, дефіцитні товари і вже звичні для молодших поколінь - електронні гроші (комп'ютерна крипто-валюта).

Із розвитком електронних систем, неодноразово виникали ідеї створити електронний аналог готівки для віддаленої оплати. Першою проблемою стала потенційна можливість подвійного витрачання одних і тих самих засобів. Підчас оплати готівкою подвійного витрачання ніколи не виникає через те, що оплата супроводжується передачею грошей і покупець не може ще раз їх заплатити іншому продавцю, адже у нього цих грошей вже немає. Наразі, електронним системам органічно притаманна можливість копіювання їх стану, що дозволяє відтворити повну та ідентичну копію та потім зробити кілька платежів з одного і

того самого стартового стану, тобто витратити одні і ті ж засоби в різних напрямках. Все вирішилося лише за допомогою довірених посередників, які ведуть облік платежів і гарантують оплати виключно в рамках наявності коштів, та/або кредитного ліміту. Саме так працюють всі системи безготівкових платежів. Традиційно посередниками виступають банки або інші оператори платіжних систем.

Урешті-решт, потрібно згадати такий термін, як: «криптовалюта» — це вид цифрової валюти, емісія та облік якої засновані на асиметричному шифруванні і застосуванні різних криптографічних методів захисту системи. Дана технологія була розроблена для того, щоб запобігти участі посередників. Вирішили це в системі «біткойнів», за рахунок штучного ускладнення внесення змін до реєстру історії операцій.

Біткойн — це пірінгова платіжна система, яка використовує однойменну одиницю для обліку операцій. Для забезпечення функціонування і захисту системи використовуються криптографічні методи, але при цьому вся інформація про транзакції між адресами системи доступна у відкритому вигляді. Біткойни можуть використовуватися для обміну на товари або послуги у продавців, які згодні їх приймати. Обмін на звичайні валюти відбувається через онлайн-сервіс обміну цифрових валют, інші платіжні системи, обмінні пункти або безпосередньо між зацікавленими сторонами. Написаний був на мові програмування «C++» у 2009 році.

Однією з головних особливостей системи є повна децентралізація: немає центрального адміністратора або будь-якого його аналога. Необхідним елементом цієї платіжної системи є - базова програма-клієнт. Запущені на безлічі комп'ютерів дані програми обмінюються між собою інформацією та об’єднуються в однорангові з'єднання, кожен вузол якої рівноправний і самодостатній. Неможливо державне чи приватне управління системою, в тому числі зміна сумарної кількості біткойнов. Заздалегідь відомі обсяг і час випуску нових біткойнів, але розподіляються вони відносно випадково серед тих, хто використовує своє обладнання для обчислення. Відсутність у криптовалюти будь-якого внутрішнього або зовнішнього адміністратора призводить до того, що банки, податкові, судові та інші державні або приватні органи не можуть впливати на транзакції будь-яких учасників платіжної системи. Передача криптовалюти незворотна - ніхто не може скасувати, заблокувати, оскаржити або примусово (без приватного ключа) здійснити транзакцію.

Для зберігання інформації транзакції об'єднуються в блоки, з яких формується безперервний ланцюжок «blockchain». Блокчейн - вибудуваний за певними правилами безперервний та послідовний ланцюжок блоків, які містять інформацію. Найчастіше копії ланцюжків блоків зберігаються на безлічі різних комп'ютерів незалежно один від одного. Концепція технології блокчейн запропонована Сатоши Накамото в 2008 році, а вперше застосована на практиці при появі біткойна в 2009-му. Через походження її відносять до транзакцій криптовалют, але сфера застосування технології помітно ширше. Система працює наступним чином: створюється первинний блок, в ньому відсутній запис про попередній блок. Кожен наступний блок містить інформацію про попередній блок, у вигляді транзакції, власному заголовку, використовуваному при генерації чергового блоку. Користувачі системи бачать всю кількість блоків, але володіють доступом лише до своїх.

Перспективи розвитку блокчейн-технологій пов'язані з активним розвитком хмарних сервісів, включаючи онлайн-банкінг, інтернет-каталоги, системи ідентифікації входу на корпоративні сайти. З огляду на те, як працює блокчейн, за запропонованою схемою працює криптовалюта, як популярний біткоіни, так і його аналоги, але цим сфери застосування не обмежуються. Великий інтерес розподіленої системи зберігання даних для банківських установ, державних організацій, що надають загальний доступ до баз даних на зразок медичних карт, пенсійних нарахувань…

Щодо перспективних напрямків використання блокчейн-систем: право володіння (авторство); операції з сировиною, товаром; перевірка справжності, підтвердження прав доступу, управління даними, засоби електронного голосування, онлайн ігри. Переважний перехід приватних та державних компаній на інтернет-технології дає можливість інтеграції блокчейнов в існуючу інфраструктуру без видимих перетворень. Впровадження можливо шляхом зміни внутрішніх алгоритмів зберігання даних, надання доступу до них з боку користувачів. Якщо залишити колишній інтерфейс, власники особистих кабінетів навіть не помітять різниці, відчувши лише помітно зросла швидкість роботи ресурсу.

Розглянемо курс біткоіна починаючи з 2012 року по 2020: його ціна піднялась навіть з 0 до 42000 доларів. Зараз подивимося від чого залежить його ціна. Перша причина - попит і пропозиція, як головне правило економіки. По-друге, «майнінг біткоіна» - це енергоємний процес, і тому виробництво монет

пов'язано зі значними витратами. Для роботи майнінгового обладнання потрібно багато електроенергії, так як ці машини вирішують багато завдань для того, щоб добути черговий блок.

Ми не змогли б купувати або продавати біткоіни, якби їх не було на біржах. Купівля біткоінів на крипто-біржах - це найпростіший спосіб отримати монети. Якщо доступність монет на біржах знизиться, то і покупка біткоіни буде утруднена, що призведе до зростання ціни.

Біткойни залишаються найбільш домінуючою криптовалютою в світі. Однак, якщо конкуренція серед криптовалют почне загострюватися, то можна очікувати, що капіталізація ринку біткоінів зменшиться, і гроші почнуть іти на ринок альткоінов. Це може зробити негативний вплив і на ціну біткойнів.

У програмний код біткоінів закладено жорстке обмеження на максимально можливу кількість монет - 21 мільйон одиниць. Блокчейн встановлює правило - кожні 4 роки винагороду за знайдений блок зменшується в 2 рази, тобто емісія нових монет сповільнюється. Це зроблено з метою підвищення вартості монет.

Далі хочу розглянути спосіб, як можна займатися майнінгом: майнінг, також видобуток - діяльність по створенню нових структур для забезпечення функціонування кріптовалютних платформ. За створення чергової структурної одиниці зазвичай передбачено винагороду за рахунок нових одиниць криптовалют або комісійних зборів. Як приклад використовуються обчислення хешів, аналогічні обчисленням в системі біткойнів, де процес Майнінга полягає в підборі такого значення спеціального додаткового параметра Nonce, яке дозволить отримати хеш, числове значення якого буде не більше деякого заданого числа - Difficulty Target, цільового при даному рівні складності.

Система біткойнов передбачає тільки одну можливість для додаткової емісії - нові біткойни отримує в якості винагороди той, хто згенерував черговий блок. Отриману винагороду за блоки можна використовувати після отримання 120 підтверджень (тобто мережа дозволяє витрачати винагороду приблизно через 20 годин). Імовірність отримання нагороди соло-майнер в довільний десятихвилинний період приблизно дорівнює співвідношенню його обчислювальної потужності до обчислювальної потужності всієї мережі і якщо це співвідношення дуже маленьке, то ймовірність отримання нагороди навіть за тривалий проміжок часу також буде низькою.

Бажають отримати якомога більшу винагороду прагнули задіяти якомога більші обчислювальні потужності.

Як можна займатися майнінгом вдома? Кріптовалютний ринок великий, але якщо ви не хочете ризикувати - вибирайте перевірені роками монети. До стабільних, перспективних, потрібних і дохідним криптовалютам можна віднести: Bitcoin, Monero, Zcach, Dash, Litecoin і звичайно ж Ethereum. Для початку роботи з криптовалютой - вам буде потрібно завести гаманець. Якщо мова йде не про зберігання - можна скористатися bitcoin гаманцем від moneypipe.

Так, як поодинці добувати криптовалюта без великих потужностей не вийде, то домашні Майнер часто об'єднуються в пули. Це кілька машин, які об'єднують свої зусилля для пошуку необхідного блоку. Після того, як цей блок буде знайдений, винагорода розподіляється згідно потужностям.

Тепер до питання про можливий заробіток зі звичайним комп'ютером. Для сучасних криптовалют потрібні потужності, які може видати тільки одна деталь комп'ютера - відеокарта. Про видобуток криптовалюта на процесорі і жорсткому диску можете забути. І тому те, скільки ви отримаєте за день безпосередньо залежить від потужності вашої відеокарти. На 2021 рік найкращою відеокартою буде Nvidia RTX 2080ti (ціна в Україні від 30 до 60 тисяч гривень).

Карта у непотужному режимі роботи приносить близько $ 1 в день. Якщо розігнати і підключити обладнання, то показник буде приблизно $ 1.7 / день при належному везінні. І це якщо комп'ютер буде працювати 24 \ 7. Погодьтеся, не найбільш вражаюча цифра до порівняння скільки коштує потужне обладнання, та ще за світло платити.

Якщо брати біль бюджетне обладнання то цифри будуть ще менші, на прикладі свого ноутбука – відеокарта nVidia GeForce GTX 1050, я користувався програмою від Kryptex і по тестам вона підійшла, але насправді, ця карта була актуальна у 2018 році і для майнінга валюти Etherium і з моєї відеокарти можна мати максимум 0,25$ у день і то не факт, що вийде.

Розігнати відеокарту не так вже й просто. Можливості і продуктивність в сфері майнінга іноді можуть бути не залежними один від одного. Можна майніти і при обмеженні споживання в 75%. Менше, всього лише на половину хешрейта від всієї потужності. За рахунок цього знижується нагрів і можна заощадити кілька сотен гривень за місяць, на кожній фермі GTX.

Визначивши хешрейт, можна розрахувати повністю термін окупності вашої карти на сервісі Whattomine - http://whattomine.com/calculators. Додатково необхідно вказати

ціну за електрику і потужність пристрою. Сервіс періодично оновлює інформацію (включаючи збільшення рівня складності, зниження плати за розшифровку блоків), тому про актуальність даних можна не турбуватися.

Далі я дізнався, чому не потрібно займатися майнінгом на ноутбуках. У 2010-2011 роках, можна було добувати криптовалюта практично на всьому. Напевно, десь знайшлися б умільці, які змогли б зробити ферму з тостерів. Але зараз все дуже змінилося. Майнер стало багато, алгоритми ускладнилися і тепер для того, щоб добувати 1 біткоін в день потрібно комп'ютер божевільною потужності. На ноутбуці Майнінг невигідний. Від слова зовсім. Особливо зараз, зі стрибком долара, техніка стала дійсно дуже дорогою, приклад мого ноутбука – минулого року я взяв у магазині його за 22000, зараз він без акції коштує від 25 до 36 тисячи гривень.

Ризики криптосистем: поряд з очевидними перевагами на практиці робота криптосистем не бездоганна і виявляє ряд серйозних недоліків. Перша проблема пов'язана з обмеженою пропускною потужністю платіжної системи. Звернення криптовалюта на основі блокчейна включає двох основних учасників - Майнер і користувачів. Майнер служать бухгалтерами і підтримують системну інфраструктуру шляхом оновлення списку транзакцій. Користувачі здійснюють і отримують платежі. Фінансовим стимулом роботи Майнер є збори, що стягуються з користувачів за постановку в чергу на проведення транзакцій. Щоб генерувати призначені для користувача збори ємність системи повинна бути досить невеликий.

Наприклад, пропускна здатність через систему Visa становить 3526 транзакцій в секунду, в той час як через систему Bitcoin - 3,3 транзакції. Обмеження потужності перевантажують систему, особливо в години пік, і ведуть до зростання комісії. Наприклад, в грудні 2017 р плата за обробку платежу зросла до 57 доларів за транзакцію, незалежно від її призначення. Друга проблема - відсутність гарантій остаточності платежів. Платіж, записаний в бухгалтерську книгу, не гарантує, що він є остаточним і безвідкличним. Криптовалюта тримаються на угоді між Майнер. Якщо частина з них змовиться і вирішить переписати історію транзакцій, платіж може бути знищений. Зокрема, подібний прецедент був створений на найбільшій японській біржі біткоіни Mt. Gox. У лютому 2014 року ця біржа оголосила банкрутство після пропажі 850 тис. Біткоінових монет вартістю в півмільярда доларів, що дещо послабило віру користувачів в досконаліть роботи криптосистем. Третя

проблема - Обчислювальна потужність окремих майнерскіх ферм, на яких видобуваються криптовалюта, еквівалентна потужності мільйонів персональних комп'ютерів. Загальний обсяг електроенергії, що витрачається на видобуток біткоіни в середині 2018 дорівнював витратам електроенергії такої середньої за величиною країни, як Швейцарія. Інші криптовалюта також використовують досить багато електрики. Такі обсяги споживання енергії можуть швидко перетворитися в екологічну катастрофу. Четверта проблема криптовалюта пов'язана з їх надзвичайної волатильністю, що обумовлено відсутністю центрального емітента, покликаного гарантувати вартісну стабільність за допомогою використання різних інструментів монетарної політики.

Як висновок, хочу сказати, що якщо ви маєте потужне обладнання, гроші, які не страшно втратити на майнінг, не дуже турбують глобальні проблеми від криптовалюти, то звісно можна ризикнути, я спробував та не залишився задоволеним.

Література:

1. *https://miningbitcoinguide.com/mining/sposoby/na-domashnem-pk#____2019*
2. *https://altcoinlog.com/mayning-na-videokarte*
3. *https://russiancouncil.ru/analytics-and-comments/analytics/kriptovalyuty-i-budushchee-globalizatsii/*
4. *https://bitnovosti.com/2020/03/19/budushhee-kriptovalyuty/*
5. *https://www.kryptex.org/site/dashboard (Програма, яку я використовував для майнінга)*
6. *alpari.com*
7. *ru.wikipedia.org*
8. *Поппер Н. Цифровое золото: невероятная история Биткойна. М.: ООО «И.Д. Вильямс», 2016.*

НАЙБІЛЬШ «ГУЧНІ» ВИТОКИ ДАНИХ І ВЗЛОМИ 2020 РОКУ

Шулімова Дар'я Денисівна
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

2020 рік був одним з найгірших для кібербезпеки. У світлі пандемії і катастрофічних економічних потрясінь, турбота про збереження нашої особистої конфіденційності та безпеки в Інтернеті пішли далеко від наших пріоритетів.

Дослідники за 2020 рік зафіксували величезний сплеск фішингових атак на банківський сектор. Медичні компанії з початком розробки вакцини від «той кого не можна називати» потрапили під приціл хакерських угруповань.

Що стосується витоку даних, то в 2020 році було зламано більше 737 мільйонів файлів. Найбільша витік стався в косметичній компанії Estee Lauder, 440 мільйонів записів «витекли» в руки до хакерів.

Компанія AV-test, яка каталогізує нові види шкідливих програм, зафіксувала стрімке зростання нових типів шкідливих програм. Різке збільшення кількості атак з використанням кріптоджекінга, програм-вимагачів і фішингових атак зросла на 252% в порівнянні з минулим роком.

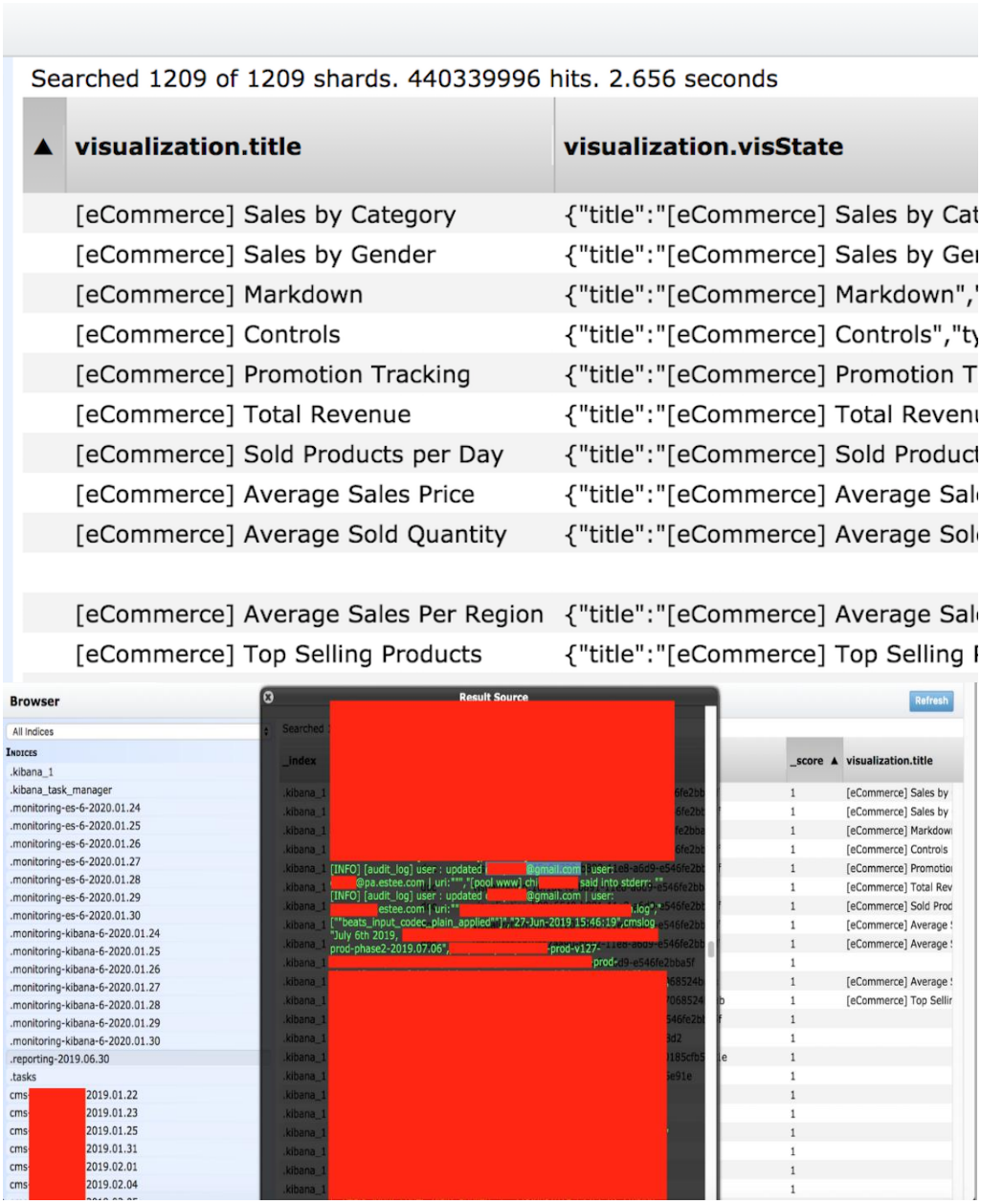
Найбільш «гучні» зломи:

Estee Lauder

Однією з найсерйозніших витоків даних за рік можна назвати компанію Estee Lauder. Витік даних виявлена в лютому 2020 року. У Транснаціональної косметичної компанії «повели» 440 мільйонів записів. З 440 цільових файлів невизначену кількість включали адреси електронної пошти клієнтів зберігається як звичайний текст.

Всі викрадені дані злочинці вивантажили на відкритих ресурсах інтернету. Незахищена паролем база даних була виявлена в кінці січня дослідником безпеки Джеремі Фаулером. Неясно, яким методом хакери взяли інформацію і як довго вона була доступна. Як пише в своєму звіті дослідник Джеремі Фаулер у виявленій базі даних перебувало:

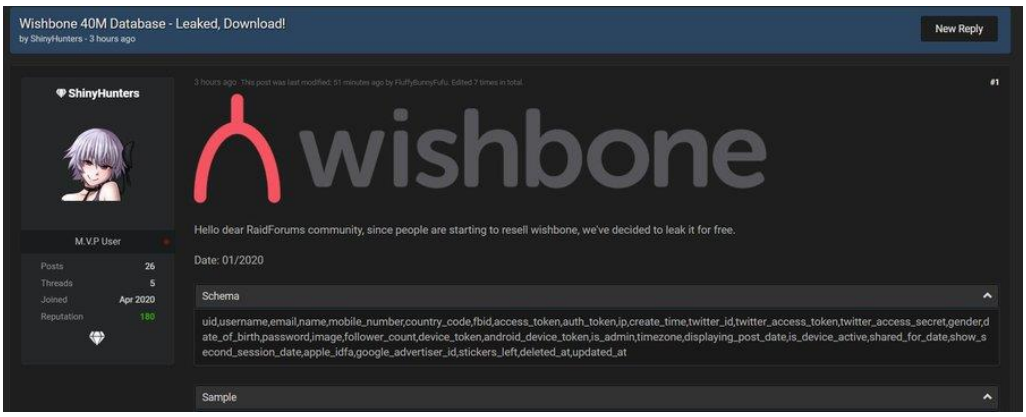
- 440 336 852 записів.
- «Користувацькі» електронні листи у вигляді звичайного тексту (включаючи внутрішні адреси електронної пошти в домені @ estee.com)
- Були відкриті журнали виробництва, аудиту, помилок, CMS та проміжного програмного забезпечення.
- Посилання на звіти та інші внутрішні документи.
- IP-адреси, порти, шляхи і інформація про сховище, які кіберзлочинці можуть використовувати для більш глибокого доступу в мережу.



Розслідування проникнення до сих пір триває.

Wishbone

У додатку Wishbone в травні 2020 року стався витік 40 мільйонів для користувача записів. Хакерська група ShinyHunters виставила дані на продаж на RaidForum, популярному ринку продажу вкрадених даних, за 0,85 біткойнів (~ 8000 доларів США на той момент).



Це другий великий інцидент для Wishbone за останні три роки. У 2017 році хакери зникли з 2,2 мільйонами адрес електронної пошти і майже 300 000 номерів телефонів.

Багато з них належали жінкам. Документи, які просочилися приблизно в той же час, показали, що більше 70% користувачів Wishbone були молодше 18 років.

Нове порушення периметра інформаційної безпеки зачіпає майже в 20 разів більше користувачів і включає набагато більше даних по кожному з них.

Каталін Чімпану з ZDNet повідомляє, що зламані дані включають імена користувачів, адреси електронної пошти, номери телефонів і інформацію про місцезнаходження. Він також включає хешировані паролі.

Хоча той факт, що паролі не зберігалися у вигляді звичайного тексту, є гарною новиною, Чімпану каже, що ті дані, які були досліджені, були хешировані з використанням алгоритму MD5. MD 5 був оголошений експертами «криптографічно зламаним» ще в 2010 році.

Хоча Wishbone в останні роки не розкриває загальна кількість користувачів, додаток вже багато років входить в топ-50 найпопулярніших додатків для соціальних мереж в iOS App Store, досягнувши піку в 2018 році, коли воно увійшло в десятку кращих в категорії. У магазині Google Play у додатки від 5 до 10 мільйонів завантажень.

Література:

1. https://habr.com/ru/post/535878/

ЗАСОБИ І МЕТОДИ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ ТЕХНІЧНИХ КАНАЛІВ ВИТОКУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Якубенко Володимир Володимирович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише їх формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу.

Розвиток теорії інформації сигналів та радіоелектроніки, призвели до виникнення інформаційного суспільства. Основою такого суспільства є інформаційні технології та інформація, яка в таких умовах стає товаром й основним продуктом виробництва та створення додаткової вартості.

Зворотнім боком цієї "медалі" є тотальні незаконні зазіхання на чужу інформацію, що, в свою чергу, вимагає її захисту. Особливу небезпеку складають спроби викрадення інформації, що є власністю держави та містить державну або іншу таємницю.

Ключові слова: виток інформації, конфіденційні дані, середовище сигналів, кібербезпека.

Отже, для розуміння принципів технічного захисту інформації треба знати способи і засоби її зняття, оцінити реальність загроз використання для цього різних каналів.

На рис. 1 наведено практично всі методи та засоби комбінованого зняття акустичної інформації: спочатку вказано канал витоку, а потім можливі способи та засоби зняття інформації. Відповідно до розташування та облаштування об'єкту, що охороняється, можливо використання різних каналів витоку. При цьому можуть використовуватися різні види перетворення та способи і засоби перенесення інформації. Наприклад, акустичну інформацію можна зняти в приміщенні за допомогою радіомікрофону, який живиться від струму електромережі, а можна виконати цю операцію за допомогою дротового мікрофону, який також підключено до електромережі. В цьому випадку інформація буде передаватися електромережею і її можна зняти навіть на трансформаторній підстанції.

Для зняття акустичної інформації з закритого приміщення дедалі частіше використовується так зване ВЧ-нав'язування, коли для зняття інформації використовується будь-який "цінний" подарунок (наприклад, картина або естамп), виконаний так, що він стає резонансним елементом модуляційної системи. При ВЧ опромінюванні цього елементу відбувається модуляція мовними сигналами спрямованого на цей елемент високочастотного радіовипромінювання. Таким самим чином, розрахувавши або експериментально з'ясувавши резонансні характеристики дзвінкового кола телефонного апарату чи, наприклад, трансформаторного кола радіоточки, можна зняти мовну інформацію за допомогою ВЧ-нав'язування.

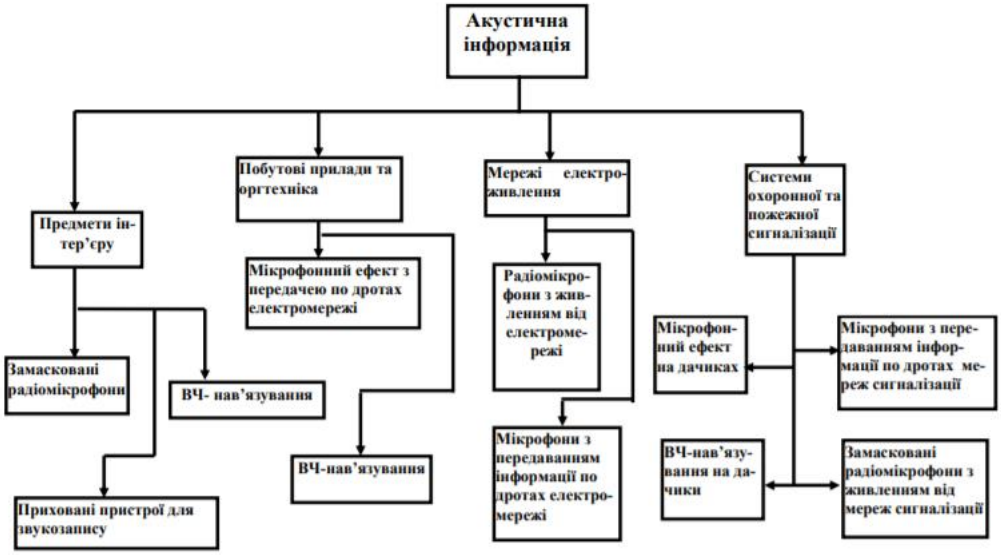


Рис. 1 – Комбіновані методи та засоби зняття акустичної інформації

В закритих приміщеннях акустичну інформацію можна знімати за рахунок того, що будівельні конструкції (стіни, підлоги, стелі, вікна, труби, зачинені двері) є по суті акустичними мембранами та чудово передають звукові коливання.

Таким чином, за допомогою віброперетворювача та підсилювача можна знімати акустичний сигнал з будь-якого приміщення через стіну, підлогу або стелю.

На відстані акустичний сигнал можна зняти з зачинених вікон, спрямувавши випромінювання лазеру на скло чи скористувавшись спрямованим мікрофоном.

Акустичну інформацію можна знімати також з побутових приладів та апаратури зв'язку.

Особливо небезпечним приладом є телефон. Наявність незахищеного телефонного апарату в режимному приміщенні дає змогу без зайвого клопоту прослухувати в ньому всю акустичну інформацію навіть не використовуючи радіомікрофони чи іншу дорогу спецтехніку. При чому це можна робити навіть тоді, коли трубка лежить на апараті, тобто телефон, здається, виключено. Але дзвінкове коло телефону має елементи, що створюють резонансний контур, який постійно підключений до телефонної мережі під напругу від 40 до 60 В. Частина з них ще й мають властивості мембрани, яка коливається під дією акустичного сигналу, тобто механічних коливань повітря. При коливаннях такої мембрани відбувається зміна резонансних характеристик контуру (мікрофонний ефект). При розмові у разі наявності такого "шпигуна" на резонансному контурі відбувається модуляційний процес звуковими

коливаннями мови, тобто акустичний сигнал перетворюється в електричний. Цей сигнал надходить до дротів телефонної мережі, звідки його можна зняти за допомогою простого пристрою. Не говорячи вже про застосування ВЧ нав'язування або зняття сигналів за допомогою індукційного датчика, чи датчика з високим вхідним опором, які можна підключити до лінії зв'язку за межами приміщення чи, навіть, об'єкту, які взагалі надзвичайно важко ви- 57 явити (практично неможливо без застосування спеціальних приладів, що вимірюють неоднорідність мережі).

Мають свої резонансні контури та мембранні елементи інші побутові прилади: кондиціонери, оргтехніка (наприклад, електрична друкарська машинка). В цьому випадку акустичну інформацію можна зняти з електричної мережі, до якої вони підключені. Нарешті, завжди існує загроза встановлення радіомікрофону (інколи його звуть радіозакладним пристроєм чи радіозакладкою, або "жучком").

З розгляду способів та засобів зняття акустичної інформації видно, як багато загроз для викрадення цього виду інформації надає сучасна техніка. Але, нажаль, крім акустичної інформації, сучасна техніка перехоплення надає можливості знімати електронну чи електромагнітну інформацію, тобто фактично викрадати будь-які документи, що створюються, передаються та зберігаються у незахищених засобах електронної обробки інформації.

Література:

1. Васильєв В.І. Інтелектуальні системи захисту інформації / В.І. Васильєв - М .: МІФІ, 2017. - 201 с.

2.uk.wikipedia.org // Технічний захист інформації // листопад 26, 2019. URL: https://www.wikipedia.org/wiki/Технічний_захист_інформації.

3. Остапов С.Е., Євсеєв С.П, Король О. Г. Кібербезпека: сучасні технології захисту / Новий світ – 2000 : Наш формат, 2020. – 678 с.

4. Jeff Kosseff. Cybersecurity Law / Jeff Kosseff – Wiley. 2020 - 768 с.

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОРПОРАТИВНІЙ ІНФОРМАЦІЙНИЙ СИСТЕМІ

Ярчук Андрій Андрійович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

З кожним днем сучасні технології розвиваються ще більш стрімкішими темпами, а тому розробникам доводиться шукати нові способи якісного захисту інформаційних технології. В сучасних умовах розвитку науково-технічного прогресу постійно зростає обсяг оброблюваних інформаційних

ресурсів. Результати теоретичних і експериментальних досліджень, говорять про те, що зростання обсягів переданих даних збільшується пропорційно зростанню валового продукту.

Перехід на електронні форми зберігання і передачі інформації, активне впровадження в повсякденне життя електронних форм вплинули на те, що безпека мереж і мережевих сервісів стала дійсно нагальною проблемою практично всіх організацій.

Корпоративні дані в трьох випадках можуть бути вкрадені, модифіковані, знищені:

− всередині локальної мережі співробітниками навмисно або ненавмисно;

− стороння особа проникне в локальну мережу ззовні;

− стороння особа перехопить інформацію в глобальній мережі по шляху її від одного підрозділу до іншого.

Всі перераховані вище випадки можуть завдати значної шкоди компанії. Тому продумана і добре організована система безпеки дозволяє уникнути або звести до мінімуму втрату важливих даних організації.

Таким чином, виявлення вторгнень – один з ключових компонентів комплексної системи захисту. Вони дозволяють збільшити безпеку мережі, контролюючи всі вхідні і вихідні потоки трафіку, як всередині периметра, що захищається організації (відстежуючи за різними оцінками від 70 до 80% порушень, пов'язаних з внутрішніми зловмисниками), так і зовні (виявляючи спроби віддалених вторгнень і збираючи статистику невдалих проникнень).

У цій статті я дослідив сучасні технології виявлення вторгнень як засобу забезпечення інформаційної безпеки організації та особливості реалізації системи виявлення вторгненнь корпоративної інформаційної системи, також розробив рекомендації щодо застосування захисних механізмів систем IDS.

Один з основних факторів високого рівня безпеки – виявлення і припинення спроб несанкціонованого доступу в реальному масштабі часу. Як правило, в повному обсязі це необхідно тільки дуже великим мережам, але створити добре захищену мережу без засобів, що дозволяють виявляти і припиняти загрози просто неможливо. Виявлення вторгнень – один з ключових компонентів комплексної системи захисту. Вони дозволяють збільшити безпеку мережі, контролюючи всі вхідні і вихідні потоки трафіку, як всередині периметра, що захищається організації (відстежуючи за різними оцінками від 70 до 80% порушень, пов'язаних з внутрішніми зловмисниками),

так і зовні (виявляючи спроби віддалених вторгнень і збираючи статистику невдалих проникнень).

Система виявлення вторгнень є програмною або апаратною системою, яка автоматизує процес перегляду подій, що виникають в комп'ютерній системі або мережі, і аналізують їх з точки зору безпеки. Відповідний англійський термін - Intrusion Detection System (IDS). Виявлення вторгнень є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі, і аналізу їх. Вторгнення визначаються як спроби компрометації конфіденційності, цілісності, доступності або обходу механізмів безпеки комп'ютера або мережі. Системи виявлення є програмними або апаратними пристроями, які автоматизують процес моніторингу та аналізу подій, що відбуваються в мережі або системі, з метою виявлення вторгнень. Такі системи складаються з трьох функціональних компонентів: інформаційних джерел, аналізу та відповіді. Виявлення вторгнень може бути визначено як: ідентифікація комп'ютера або мережевих ресурсів для зловмисних намірів та поведінки і відповідь на процес. Система виявлення може виявляти спроби несанкціонованого проникнення у системний об'єкт або поведінки при моніторингу ліцензіатів незаконної роботи системних ресурсів.

Система виявлення вторгнень складається з трьох модулів:

- Модуля збору інформації;
- Модуля аналізу інформації;
- Модулів сигналізації і відповіді.

Двома основними підходами до аналізу мережевої активності, на сьогоднішній день є статистичний і сигнатурний. Системи виявлення вторгнень, використовує статистичний підхід після установки «навчаються» адміністратором, який задає політику системі, відповідну нормальної активності в мережі – типи трафіку, з'єднання між вузлами, використовувані протоколи і порти. При виявленні аномалій в роботі мережі або статистично значущих відмінностей трафіку від типового в даній мережі, система сповіщає про це адміністратора. Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибно позитивних тривог в разі некоректно заданих правил.

Сигнатурні системи виявлення вторгнень аналізують трафік в мережі і порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). Такий підхід схожий з тим, як працює більшість антивірусного програмного забезпечення. При такому підході основною проблемою є старіння баз сигнатур між

проявами нових типів атак і оновленням баз сигнатур може пройти достатню кількість часу, протягом якого система буде нездатна виявити таку загрозу.

Одними із головних проблем та недоліків системи виявлення вторгнень слід вважати:

Шум може серйозно вплинути на ефективність роботи такої системи. Пакети, помилково згенеровані недоліками в розробці програмного забезпечення, пошкоджені дані служби доменних імен можуть створити досить високий коефіцієнт помилкових тривог.

Старіння бібліотек сигнатур, що може серйозно позначитися на ефективності виявлення і запобігання атак. Система виявлення вторгнень не може компенсувати недоліки в проектуванні інфраструктури безпеки, уразливості протоколів як таких або слабкі методи аутентифікації.

Зашифровані пакети не обробляються системами виявлення вторгнень. Таким чином, атака з використанням зашифрованих пакетів може привести до успішного вторгнення, що не виявлену систему, поки зловмисник не почне робити дії всередині мережі, які виявляються системою.

Системи виявлення вторгнень предоставяе інформацію про атаки використовуючи мережеву адресу, що міститься в IP-пакетах, що проходять в мережі. Це ефективно, якщо мережеву адресу в пакеті справжній, так як як адреса в пакеті може бути спотворений або сфальсифікований.

Так як мережеві системи є мережевими пристроями, вони схильні до тих же протокол-орієнтованим атакам, що і звичайні вузли. Спотворена інформація і атаки на стек TCP/IP можуть привести до відмови в роботі такої системи.

Фізичне виявлення вторгнень-це акт виявлення загроз для фізичних систем. Прикладами фізичного виявлення вторгнень є:

- Охоронець;
- Камери безпеки;
- Системи контролю доступи (карти, біометрія);
- Брандмауер;
- Датчики руху.

IDS бездротової локальної мережі (wireless local area network (WLAN)) аналогічний NIDS, оскільки він може аналізувати мережевий трафік. Тим не менш, він також проаналізує трафік, специфічний для бездротової мережі, включаючи сканування точок доступу (access points (AP)), фальшивих точок доступу, користувачів за межами фізичної області компанії і WLAN IDS, вбудованих в точки доступу.

Якщо ви розгортаєте мережу IDS, ви повинні заздалегідь вирішити, де розмістити датчики моніторингу. Це буде залежати від того, яке вторгнення або яку спробу вторгнення ви намагаєтеся виявити. Треба почати із створення докладної мережевої діаграми, якщо у вас її ще немає.

Рішення про розміщення IDS в мережі досить відповідальне. Машина IDS повинна підключатися до порту, який може бачити весь трафік між локальною мережею(LAN) і Інтернетом.

Після успішної установки, вказуючи веб-браузеру на IDS, ви отримаєте вікно попереджень.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Яцко Віра Вячеславівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Метою статті «Методи захисту інформації» є вивчення методів і засобів захисту інформації у системах її створення та зберігання, системах зв'язку, в мережах обміну інформацією. А саме, вивчення:

- Загальних принципів організації захисту інформації в телекомунікаційних системах на базі сучасних концепцій.
- Принципів побудови та функціонування професійних пристроїв несанкціонованого знімання інформації у телекомунікаційних системах.
- Принципів побудови та функціонування професійних технічних пристроїв захисту інформації в телекомунікаційних системах.
- Принципів побудови та функціонування програмних засобів захисту інформації в телекомунікаційних системах нормативно-правової бази захисту інформації в Україні.
- Методів та засобів захисту інформації, методик створення та обслуговування систем захисту, технічних каналів витоку інформації.

У статті розгядаються наступні питання:

- Основи інформаційної безпеки і захисту інформації
- Основні концептуальні положення системи захисту інформації
- Сучасна постановка проблеми захисту інформації. Поняття «Інформаційна безпека». Місце, цілі і завдання інформаційної безпеки.

- Концептуальна модель інформаційної безпеки. Цілі переслідувані джерелами загроз. Прояв загроз інформації. Класифікація загроз.
- Дії, що призводять до неправомірного оволодіння конфіденційною інформацією і їх класифікація. Розголошування. Витік. Несанкціонований доступ. Формальні та неформальні канали поширення інформації.
- Забезпечення інформаційної безпеки. Основні принципи забезпечення інформаційної безпеки. Напрями захисту інформації.
- Правові основи захисту інформації. Структура законодавства України в області захисту інформації.
- Організаційні заходи захисту інформації. Організаційно-правові форми захисту інформації.
- Інженерно-технічний захист. Класифікація інженерно-технічний захисту.
- Класифікація і основні характеристики технічних каналів просочування інформації:

1. Акустичні і віброакустичні канали просочування мовної інформації
2. Знімання інформації з використанням закладних пристроїв. Загальні характеристики і побудова закладних пристроїв.

- Методи і способи захисту інформації:

1. Виявлення каналів просочування інформації
2. Захист мовної інформації.

Література:

1. Омельянов В.В., Курейчик В.В., Курейчик В.М. «Теорія і практика волюційного моделювання». 2003, 432 ст.

2. Таха Х.А. «Введення в дослідження операцій», 2005, 912ст.

3. Вагнер Г.О. «Основи дослідження операцій». 1972 – 1973, 316 ст.

4. Зуховицький С.І., Радчик І.А. «Математичні методи планування мереж». 1965, 296 ст.

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Яцко Віра Вячеславівна
Державний університет телекомунікацій
Навчально-науковий інститут Захист інформації
м. Київ

Інформаційна сфера, активно впливає на політичну, економічну, оборонну складові національної безпеки України. У сучасному світі відбувається безперервна боротьба за контроль над інформаційними потоками. Виграє той, хто не лише їх

формує та вміє регулювати у своїх власних інтересах, але й здатний забезпечити цілісність свого інформаційного ресурсу. Незаконне зазіхання на чужу інформацію, вимагає її захисту. Особливу небезпеку складають спроби викрадення інформації, що є власністю держави та містять державну або іншу таємницю. Таким чином виникла нова наука - інформаційна безпека держави. Вона поєднує у собі як загальнодержавну нормативно-правову організаційну складову, так і складові криптографічного та технічного захисту інформації.

В свою чергу криптографічний та технічний захист інформації містить питання організації, розробки та використання відповідних для цих аспектів інформаційної безпеки методів та засобів захисту. Ці складові відносяться до технічного аспекту інформаційної безпеки Знання цих каналів і способів необхідні для захисту інформації, і для блокування каналів витоку інформації.

Інформаційна безпека – захищеність (стан захищеності) основних інтересів особистості, суспільства і держави в сфері інформації, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію Інформаційна безпека є складовою національної безпеки. Але особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо.

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

- розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основними напрямами державної політики у сфері ТЗІ є:

- нормативно-правове забезпечення;

- удосконалення чинних та створення нових нормативно-правових актів щодо захисту інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що належить державі;

- розроблення нормативно-правових актів щодо захисту відкритої інформації, важливої для особи, суспільства та держави;

- удосконалення правових механізмів організаційного забезпечення ТЗІ.

На теперішній час для несанкціонованого зняття інформації широко використовуються технічні канали витоку інформації (ТКВІ). Технічний канал витоку інформації – це сукупність небезпечних фізичних сигналів, серед їх розповсюдження та зберігання, об'єкту технічної розвідки й способів і засобів технічної розвідки, що можуть бути застосовані для зняття інформації з об'єкту, що охороняється.

На сьогоднішній день розповсюджені такі канали витоку інформації:

- Акустичні канали витоку інформації, куди входять також канали з акустично-електричними перетвореннями;
- Радіотехнічні канали витоку інформації, куди входять, по-перше, відкриті канали радіотехнічного зв'язку та, по-друге, канали, що утворюються за рахунок паразитних випромінювань та наводок;
- Оптичні канали витоку інформації - речовий канал витоку інформації, який визначається людським фактором.

Інформація, яка може бути об'єктом злочинних посягань:

- Оптична;
- Акустична;
- Електронна;
- Електромагнітна;
- Письмова (друкована) інформація.

Відповідно, всі види інформації мають різну фізичну природу її походження, носіїв і каналів розповсюдження та зберігання, або різні параметри одного й того ж явища, яке може бути покладене в основу для її переносу чи зберігання.

Проведення робіт з розробки, впровадженню та підтримки й перевірки працездатності системи ТЗІ на об'єкті, що охороняється, вимагає проведення певних організаційно-технічних заходів. Їх проведення призначено для забезпечення надійності захисту інформації на об'єкті. Одне з найважливіших завдань при цьому є виявлення та блокування всіх потенційних каналів витоку інформації з об'єкту. Друге завдання – це постійна перевірка працездатності та надійності функціонування системи технічного захисту. Саме в цих заходах полягає сутність ТЗІ.

Технічний захід – це дія із захисту інформації, яка передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень. Технічні заходи включають:

- встановлення за допомогою технічних засобів потенційних каналів витоку інформації та визначення методів та засобів для їх блокування;

- перевірку техніки, яка використовується, на відповідність величини паразитних випромінювань допустимим рівням;

- екранування приміщень або техніки, яка використовується;

- перемонтаж окремих мереж, кабелів та ліній зв'язку;

- застосування спеціальних пристроїв і засобів захисту;

- використання засобів активного захисту;

- перевірку адекватності та надійності функціонування застосованих технічних засобів рівню потенційних загроз.

На початку робіт з ТЗІ необхідно визначити види інформації та від якого роду загроз треба захищатися. Для цього в першу чергу визначають категорію приміщення. При цьому з'ясовують види та ступень таємності інформації, що може циркулювати у приміщенні. Далі розглядаються конструктивні особливості приміщення та умови його розташування, наявність побутової техніки та апаратури для обробки інформації, її типи та технічні характеристики. З'ясовується та враховується наявність біля об'єкту, що треба захищати, іноземних установ, автостоянок, приватних фірм (тобто місць, з яких можна організувати стаціонарне та мобільне зняття інформації). Заміряється відстань до таких місць і визначається охоронна зона, в межах якої несанкціоноване зняття інформації вважається неможливим. Це надає змогу з'ясувати типи та ступень можливих загроз та встановити відповідну категорію захисту інформації. Якщо поряд з об'єктом є іноземні установи чи фірми, де можна організувати стаціонарне зняття інформації, категорійність приміщення підвищується на один ступень. Складається акт про встановлення категорійності приміщення, в якому відбиваються всі питання, що перераховані вище. Такий акт складається представниками підрозділу з ТЗІ та членами комісії, яка призначається керівником установи, де проводяться такі роботи. Встановлення категорійності приміщення надає змогу скласти план робіт з ТЗІ, в якому визначаються обсяги та напрямки проведення робіт з ТЗІ, термін їх проведення, необхідні технічні засоби для захисту інформації на об'єкті. Ці роботи повинен проводити ліцензіант, тобто установа, яка має державну ліцензію на проведення таких робіт. Надалі всі роботи з ТЗІ проводяться ліцензіантом. Якщо в установі є підрозділ з ТЗІ, який має ліцензію на виконання всього потрібного обсягу

робіт, то ці роботи можуть проводитися таким підрозділом. При проведенні робіт з ТЗІ необхідно провести ряд заходів, зокрема:

- Визначити та змонтувати необхідні технічні засоби, що потрібні для захисту інформації на об’єкті.
- Провести необхідні вимірювання, які б підтвердили ефективність застосування обраних технічних засобів захисту та їх правильне функціонування.

Після проведення всього комплексу технічних робіт ліцензіант разом з замовником складають акт про надання об’єкту певної категорії із захисту інформації. Лише після одержання та затвердження такого акту на об’єкті можна обробляти інформацію з обмеженим доступом. Технічний захист інформації від її несанкціонованого зняття полягає в застосуванні спеціальних технічних методів її захисту, які блокують потенційні канали витоку інформації, тобто заважають спробам її незаконного отримання. Для того, щоб захищати інформацію від витоку необхідно знати потенційні канали витоку та методи їх блокування.

Під технічним каналом витоку інформації розуміють сукупність об’єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого збирається інформація про об’єкт, і фізичного середовища, де розповсюджується інформаційний сигнал. Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх розповсюдження і способів перехоплення ТЗР більш детально технічні канали витоку інформації можна поділити на:

- Радіоканали (електромагнітне випромінювання радіодіапазону);
- Електричні (засоби провідникового зв’язку та різні струмопровідні комунікації);
- Акустичні (розповсюдження звукових коливань);
- Оптичні (електромагнітне випромінювання в інфрачервоній і ультрафіолетовій частини спектру).

Деякі з цих каналів можуть бути комбінованими, тобто бути каналами витоку для декількох видів інформації. Так, скляні конструкції та вікна можуть бути каналами витоку для акустичної та оптичної інформації, але через них можна зняти також електронну та друковану інформацію. З телефонного апарату можна зняти акустичну інформацію, а також електронну та електромагнітну і т. п. Отже, для розуміння принципів технічного захисту інформації треба знати способи і засоби її зняття, оцінити реальність загроз використання для цього різних каналів. Засоби викрадення інформації можуть знаходитись серед предметів інтер’єру,

- замасковані радіомікрофони, приховані пристрої для звукозапису, замасковані радіомікрофони з живленням від мереж сигналізації,

- в стінах, підлозі, стелі, трубах опалення та водопостачання, у вікнах з передаванням по радіоканалу.

В закритих приміщеннях акустичну інформацію можна знімати за рахунок того, що будівельні конструкції (стіни, підлоги, стелі, вікна, труби, зачинені двері) є по суті акустичними мембранами та чудово передають звукові коливання. Таким чином, за допомогою віброперетворювача та підсилювача можна знімати акустичний сигнал з будь-якого приміщення через стіну, підлогу або стелю. На відстані акустичний сигнал можна зняти з зачинених вікон, спрямувавши випромінювання лазеру на скло чи скориставшись спрямованим мікрофоном. Акустичну інформацію можна знімати також з побутових приладів та апаратури зв'язку. Особливо небезпечним приладом є телефон. Наявність незахищеного телефонного апарату в режимному приміщенні дає змогу без зайвого клопоту прослухувати в ньому всю акустичну інформацію навіть не використовуючи радіомікрофони чи іншу дорогу спецтехніку. При чому це можна робити навіть тоді, коли трубка лежить на апараті, тобто телефон, здається, виключено.

Завжди існує загроза встановлення радіомікрофону (інколи його звуть радіозакладним пристроєм чи радіозакладкою, або "жучком"). Крім того, такі коливання, зважаючи на їх високочастотний характер, потрапляють через ланцюги вторинного електроживлення до електромережі. Вони у вигляді електромагнітних наводок потрапляють на всі струмопровідні частини приміщення, де розміщено електронну апаратуру. Рівень цих коливань малий. Взагалі він не перевищує рівня власних шумів апаратури, який завжди роблять як можна меншим, щоб розширити динамічний діапазон апаратури. Але навіть цього вкрай малого рівня паразитних сигналів вистачає для перехоплення інформації за допомогою сучасної чутливої апаратури для її несанкціонованого зняття. Така апаратура може бути розміщена в легковому автомобілі, який стоїть на стоянці поряд з об'єктом. Перехоплення інформації з незахищених комп'ютерів може проводитись з відстані 200 – 300 м. При перехопленні за допомогою стаціонарних потужних засобів, які розміщаються, як правило, у дипломатичних представництвах або інших стаціонарних об'єктах розвідки та контррозвідки, перехопленням може бути охоплено великий регіон. Для глобального зняття інформації з розвідувальними цілями

використовуються супутники Землі та стаціонарні пункти розвідки.

Знаючи всі основні технічні канали витоку та класифікацію способів зняття інформації, розглянемо засоби технічної протидії протиправним намаганням її отримання. Серед них особливе значення займає поняття об'єкту захисту. Об'єкт технічного захисту інформації – це будова, приміщення, окремий основний технічний засіб або їх група, об'єднана загальним призначенням, які підлягають захисту від технічних розвідок. Розглянемо всі складові поняття об'єкту захисту. Все залежить від того які, по-перше, види інформації необхідно захистити та, по-друге, у яких приміщеннях об'єкту циркулює ця інформація. Якщо це лише один вид інформації, що може циркулювати в одному або групі приміщень будівлі, виконують лише заходи з захисту цього виду інформації та певних приміщень. Якщо треба захищати велику кількість приміщень. Якщо необхідно захистити декілька видів інформації, що циркулює у приміщеннях об'єкту, то використовується комплексний захист інформації.

При цьому і сам об'єкт захисту може розміщуватися всередині іншого об'єкту, який не є в цілому об'єктом захисту інформації. Основні технічні засоби – це технічні засоби, призначені для обробки, зберігання та передавання закритої інформації. Існують і допоміжні технічні засоби та системи, призначені для обробки відкритої інформації. Але вони можуть утворювати технічні канали витоку закритої інформації. Отже, приступаючи до захисту інформації на певному об'єкті, необхідно, в першу чергу, визначити, які види інформації підлягають захисту, а, подруге, які приміщення у будівлі (або всю будівлю) необхідно захищати. Необхідно знати ступінь таємності інформації, що підлягає захисту; загрози для інформації, які можуть виходити від потенційного супротивника. Загроза для інформації – це виток, можливість блокування або порушення цілісності інформації, яка може здійснюватися під час використання технічних засобів, недосконалих з точки зору захисту інформації, або інші канали витоку інформації. Знаючі всі ці складові, можна розробляти систему захисту інформації на об'єкті. При цьому слід пам'ятати, що для кожного виду інформації та кожного виду загроз існують цілком конкретні засоби захисту та способи їх застосування, отже треба користуватися тими системами та засобами захисту, що найбільш повно відповідають потенційним загрозам для кожного з видів інформації, яку слід захищати на конкретному об'єкті. В разі комплексного захисту

необхідно розробляти підсистеми захисту для кожного окремого виду інформації, обов’язково пов’язавши їх у комплексну систему. При цьому необхідно виявити всі потенційні канали витоку інформації та забезпечити їх блокування з рівнем технічного захисту.

Література:

1. Омельянов В.В., Курейчик В.В., Курейчик В.М. «Теорія і практика волюційного моделювання». 2003, 432 ст.

2. Таха Х.А. «Введення в дослідження операцій», 2005, 912ст.

3. Вагнер Г.О. «Основи дослідження операцій». 1972 – 1973, 316 ст.

4. Зуховицький С.І., Радчик І.А. «Математичні методи планування мереж». 1965, 296 ст.

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Байбакова Карина Геннадіївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

Визначено основн інапрями державного регулювання розвитку ринкі в телекомунікаційних послуг, за рахунок створення рівних та справедливих умов діяльності для всіх суб'єктів господарювання для підвищення рівня конкуренції за вимоги технологічно нейтрального регламентування та засновані на оптимальному сполученні правових, економічних і організаційно-управлінських методів.Визначено основні роль і проблеми розвитку телекомунікацій та шляхи вирішення подолання цих проблем, вдосконалення сфери телекомунікації.

Концепція розвитку телекомунікацій в Україні до 2010 року відповідно до Закону України "Про телекомунікації" визначає основні засади і напрями подальшого розвитку телекомунікаційних мереж загального користування в ринкових умовах і спрямована на досягнення стратегічних інтересів та конкурентоспроможності України на міжнародному ринку.

Концепція визначає проблеми розвитку телекомунікацій, стратегію і основні шляхи їх розв'язання, а також принципи забезпечення комплексного розвитку телекомунікацій. Стратегія розвитку телекомунікаційних мереж повинна базуватися на використанні новітніх технологій, які відповідають міжнародним стандартам, враховувати необхідність технологічної взаємодії всіх мереж при наданні телекомунікаційних послуг, забезпечити підвищення ефективності їх функціонування.

Стрімкий розвиток інформаційних технологій зумовлює все більшу взаємозалежність соціально-економічного потенціалу держав і такого загальноприйнятого у світовому співтоваристві показника, як рейтинг розвитку інформаційно-телекомунікаційних технологій (ІКТ).

Роль і проблеми розвитку телекомунікацій

Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки

України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

У сфері телекомунікацій існують так і проблеми:

- низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;

- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загально-доступних телекомунікаційних послуг;

- наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;

- недостатній регуляторний вплив держави на ринок телекомунікацій;

- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Повільні темпи розвитку телекомунікацій спричинюють зниження конкурентоспроможності економіки та невизначність соціально-економічних проблем України, що вимагає:

- усунення нерівномірного забезпечення телекомунікаційними послугами та обмеженості доступу користувачів до загально-доступних телекомунікаційних послуг перелік яких визначається законодавством;

- прискореного розвитку телекомунікаційних мереж загального користування та збільшення переліку телекомунікаційних послуг, що надаються широким верствам населення. Для прискорення телефонізації сільських та гірських регіонів пропонується створити фонд загальнодоступних універсальних послуг за рахунок коштів якого провести телефонізацію цих регіонів;

- прискореного розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень і удосконалення державної та регуляторного впливу на ринок телекомунікацій з метою наближення його до сучасних між народних вимог.

Висновок. Таким чином, незважаючи на визначений обсяг соціально-економічних проблем, сфера телекомунікацій, яка займає значне місце в економіці країни (регіону, району), чинить значний вплив на її розвиток. Проблеми складні, однак без їх вирішення не можливий подальший розвиток телекомунікацій країни в цілому та її окремих регіонів.

Література:

1. І. Малець «РОЛЬ ТА ПРОБЛЕМИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ» с.74-75

2. І.Бенько, В.Бенько «Аналіз стану телекомунікацій в Україні та пперспеективирозвитку» с.29

3. Урядовий портал «концепціярозвиткутелекомунікацій в Україні»

4. Кузнєцова О.В., Слободянюк О.В., Урікова О.М. «Сфера телекомунікацій:соціально-економічніпроблемивпровадженняінтернет-послуг у сільськихрегіонах» с.74

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЇ

Богатиренко Дар'я Сергіївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

"Телекомунікаційний світ - це ширший термін для інформаційних технологій (IT), який відноситься до всіх комунікаційних технологій, включаючи Інтернет, бездротові мережі, мобільні телефони, комп'ютери, програмне забезпечення ,відео-конференції, аудіо-конференції, соціальні мережі та інші медіа-додатки та послуги, що дозволяють користувачам отримувати, зберігати, передавати, запам'ятовувати і маніпулювати інформацією в цифровій формі. Тому на сьогоднішній день, це найпопулярніша тема, яку обговорює кожна людина."

Телекомунікації складаються з компаній, які роблять можливим спілкування в глобальному масштабі: за допомогою телефону чи Інтернету, через ефір або кабелі, через дроти чи бездротову мережу. Ці компанії створили інфраструктуру, яка дозволяє передавати дані словами, голосом, аудіо чи відео в будь-яку точку світу. Найбільшими компаніями у цьому секторі є оператори телефонного (дротового та бездротового зв'язку), супутникові компанії, кабельні компанії та провайдери Інтернет-послуг.

Стрімкий розвиток бездротових мереж почався в 1990-х роках, коли поява цифрових бездротових мереж призвела до соціальної революції та переходу парадигми від дротових технологій до бездротових. Такий розвиток бездротових мереж змінили спосіб життя та ведення бізнесу. Сталий розвиток можливо зробити лише за умов стабільної роботи підприємств телекомунікаційної сфери, що спрямована на подальший успішний і прибутковий розвиток. Важливо, щоб підприємства телекомунікацій були динамічними, адаптивними та мали вміння швидкого реагування на стрімкий, схильний до кардинальних змін телекомунікаційний ринок. Звісно, якщо інформаційно-телекомунікаційні функції недостатньо

ефективні, то вони не зможуть поширюватисьбез налагодженого механізму управління даними послугами.

Свого часу телекомунікації вимагали фізичних проводів, що з'єднують будинки та підприємства. У сучасному суспільстві технології стали мобільними, а бездротові та цифрові технології стають основною формою спілкування. Тому зараз кожній людині легше подати різну інформацію через телекомунікаційний світ оновлених технологій. Основні державні корпорації виступають у ролі постачальників послуг, тоді як менші компанії продають та обслуговують обладнання, таке як маршрутизатори, комутатори та інфраструктура, які забезпечують це спілкування.

Досягнення бажаного рівня в телекомунікаціях неможливе без вкладу зусиль та подолання накопичених суперечностей в економіці. Сфера телекомунікацій та її підприємства як складові являють собою стратегічне значення для сталого розвитку й подальшої інтеграції усіх сфер і галузей економіки у процеси світової глобалізації. Управління підприємствами телекомунікацій – складне системне утворення й пов'язане з багатьма змінними, що сприяє виникненню проблем усередині підприємницької системи. Тому, щоб постійно мати прогрес, потрібно прикладати зусилля. Проблеми та їх накопичення, призводить спочатку до кризи, а потім – до банкрутства підприємства. Виявлення суперечностей і подальше визначення структури проблем можна представити за допомогою принципів, які повинні враховуватись керівниками й фахівцями підприємства при реалізації своєї діяльності.

Питанням дослідження суперечностей і проблем в економіці й філософії присвячено багато робіт: з точки зору системного підходу – О.О. Богданов, зарубіжних та вітчизняних економістів – це А. Файоль, Ф.У. Тейлор, Л.О.Лігоненко, А.А.Чухно, А.В.Кузьмінов, В.М.Орлов, В.М. Гранатуров, П.П. Воробієнко та ін.

Проблеми телекомунікаційних систем:

- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг(особливо у сільській та гірській місцевості);

- неефективне використання можливостей прокладених волокно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;

- недостатній регуляторний вплив держави на ринок телекомунікацій;

- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій;

- визначення джерел надходження цих коштів.

Особливостями руху телекомунікацій є те, що за допомогою людської діяльності вони дають шалений розвиток у всьому світі. Процес економічного підйому дає результат прогресу, що супроводжують розвиток виробництва і стимулюють розв'язок проблем телекомунікацій. Невирішені проблеми стають бар'єром на шляху зростання ефективності економіки, стримують занепад та поступово впроваджують нові технології. Найгострішою проблемою в Україні є суперечності, які перешкоджають задоволенню потреб. Тому головною проблемою єнедосконаліть державної політики щодо стимулювання розвитку телекомунікаційнихпідприємств.

Література:

1. Чекаліна М.А. Принципи стратегічного планування на підприємстві/ М.А. Чекаліна // Вісник ОДУ. – 2009.– № 1. – С. 83-89.

2. Економіка телекомунікацій: навч. посіб. [для студентів вищих навчальних закладів]; за заг. ред. В.М. Орлова. – О.: ОНАЗ ім. О.С. Попова, 2014. – 512 с.

3. Кравченко А.І. Історія менеджменту: підручник / А.І. Кравченко. – 3-тє вид., перероб. і доп. – М.: КНОРУС, 2010. – 432 с.

4. Чухно А. Сучасна фінансово-економічна криза: природа, шляхи і методи її подолання / А. Чухно // Економіка України. – 2010. – № 1. – С. 4-18.

ВПЛИВ ТЕЛЕКОМУНІКАЦІЙ НА ПІДПРИЄМСТВА

Виноградня Дар'я Сергіївна

Державний університет телекомунікацій ,

Навчально-науковий інститут менеджменту та підприємництва

м.Київ

Розглянуто поняття телекомунікації її розвиток та вплив у суспільсті. Встановлено вплив технологій та інновацій на підприємстві і чи потрібні вони взагалі.

Насамперед визначимо щ особою представляють телекомунікації. Телекомунікація це передача інформації через різні пристрою, яка відбувається за допомогою електрики, що проходить через фізичному носії, як-от кабель, або за допомогою електромагнітного випромінювання. Термін часто використовується в множині, тобто телекомунікації, тому що для передачі використовуються багато різних технологій.

Сучасний розвиток телекомунікаційної сфери тісно пов'язаний з інформаційними потоками та особливим значенням інформації як фактор виробництва. Галузь зв'язку

забезпечує бюджет каїни стабільними відрахуваннями та значним внеском у формування ВВП країни. Крім того, уможливлюється загальнодоступність телекомунікаційних послуг, до яких належать: підключення кінцевого обладнання споживача до телекомунікаційних мереж фіксованого зв'язку загального користування, послуги фіксованого телефонного зв'язку (місцевий та міжнароднийтелефонний зв'язок), а також виклик служб екстреної допомоги.

Виходячи з представлення про телекомунікації, розуміємо що вони однозначно впливають, оточують нас весь час, мають вплив і тим самим допомагають існувати в сучасному світі. Підприємства не є виключенням, вони ще більш тісно пов’язані з телекомунікаціями, так як вся робота тримається на зв’язках та інформації. Але не всі підприємства вміють правильно використовувати можливості телекомунікацій та не вміють пристосовуватися до швидко розвиваючими технологіям, але сама за рахунок цього підприємства можуть залишатися на плаву.

Основною метою діяльності будь-якого підприємства є отримання прибутку та його максимізація. Одним із шляхів максимізації прибутку є впровадження на підприємстві інноваційної діяльності. Головна мета інноваційної діяльності – одержання певної кількості інновацій у вигляді нової продукції, технології, сировини, методів організації та керування й т. д., що володіють певними (відповідним вимогам підприємства) характеристиками. Вони повинні орієнтуватись, з одного боку, на якнайбільш повне задоволення потреб споживачів, а з іншого – на отримання певного економічного ефекту для підприємства у вигляді прибутку.

На сьогоднішній день телекомунікаційні підприємства відіграють важливу роль як в економіці України, так і в житті кожної особистості. Варто відмітити, що частка ринку, яку вони займають з кожним роком зростає. Відповідно збільшується й сума прибутків від реалізації товарів та послуг різними за розмірами телекомунікаційними підприємствами.

Проте, варто відмітити, що в останні роки зуми збитків у середніх та малих за розмірами телекомунікаційних підприємствах є значно вищими, ніж у великих, що свідчить про необхідність підвищення їхньої конкурентоспро-можності, в першу чергу, за рахунок ефективного використання інновацій у своїй діяльності. Саме впровадження інновацій у діяльність телекомунікаційних підприємств є однією із передумов підвищення попиту на телекомунікаційні послуги та залучення нових груп споживачів.

Таким чином, у сучасних умовах соціально-економічних змін, швидких темпів розвитку науки і техніки основним засобом, що дозволяє телекомунікаційним підприємствам підвищити свій рівень прибутковості є раціональне використання їхінноваційної діяльності. Кожне підприємство прагне досягти певної конкурентної переваги на ринку за рахунок споживчої цінності товарів, продуктивності бізнесу, інноваційного потенціалу, рівня гнучкості та адаптації техніко-технологічних засобів, форм і методів управління своєю діяльністю. Стає очевидним, що лише інноваційні капіталовкладення створюють відповідні структурні зміни праці і капіталу, конкурентні умови економічного зростання та ефективності виробництва. Також інноваційні капіталовкладення поліпшують раціональне використання будь-яких ресурсів, здатні підвищувати якість та продуктивність залученої праці, вироблених товарів та наданих послуг.

Література:

1. Інноваційний розвиток промислових підприємств: аналіз та оцінки: монографія / М.П. Войнаренко та ін. Хмельницький: ХНУ, 2010. 444 с.

2.Про інноваційну діяльність : Закон України від 4 липня 2002 р. No 40-IV / Верховна Рада України. URL: http://zakon4.rada.gov.ua/laws/show/40-15.

3. Про телекомунікації: Закон України №2392-VIвід 01.07.2010 / Верховна Рада України. URL:https://zakon.rada.gov.ua/laws/show/1280-15#Text

ЗАСТОСУВАННЯ CRM В ТЕЛЕКОМУНІКАЦІЯХ

Висоцький А.Ю
Державний університет телекомунікацій
Навчально-науковий інститут Захисту інформації
м. Київ

Ефективне управління бізнесом в сучасних умовах неможливо без широкого застосування інформаційно-телекомунікаційних технологій. В умовах цифровізації економіки в системі управління компанією циркулюють великі обсяги інформації, ручна обробка якої стає практично неможливою [2]. Тому звертається особлива увага на інтелектуальний аналіз даних і впровадження CRM (Customer Relationship Management).

Специфіка діяльності телекомунікаційних компаній, перш за все операторів фіксованого та рухомого зв'язку, робота з величезними базами даних абонентів, формування пакетних пропозицій і складна система тарифікації послуг, визначають необхідність застосування різних інструментів CRM для забезпечення стратегії клієнтоорієнтованості [1-3].

Основні причини застосування інтелектуального аналізу даних, а також CRM в телекомунікаціях це: конкурентний ринок, високий відтік клієнтів, величезний обсяг баз даних.

Конкурентний ринок. Ринок телекомунікацій демонструє високий рівень конкуренції. Абонент з легкістю може перейти від одного провайдера послуг до іншого, оскільки постачальників таких послуг тепер з'явилась велика кількість. У зв'язку з цим, для досягнення високої конкурентоспроможності, телекомунікаційним компаніям варто звернути увагу на CRM рішення. Без стратегічного аналізу поточної і майбутньої ринкової ситуації, виявлення і аналізу факторів попиту, розуміння демографічних характеристик і поведінки клієнтів, телекомунікаційні компанії не зможуть успішно розробляти і коригувати свої бізнес-моделі та маркетингові стратегії, для досягнення найкращих результатів з метою підвищення лояльності абонентів і рентабельності компанії [4].

Високий відтік клієнтів. Конкурентне середовище завжди виражається у високому показнику відтоку клієнтів. Зрозуміло, що з розвитком ринку показники почали зростати. Цей факт змушує телекомунікаційні компанії сфокусуватися на своїх абонентах і знайти рішення для їх максимально тривалого утримання. Інтелектуальний аналіз даних про клієнтів допомогає спрогнозувати, коли конкретний абонент може перейти до іншого оператора послуг і чому, оцінити перспективи свого розвитку [4-5].

Величезний обсяг бази даних. Телекомунікаційні компанії збирають значні обсяги даних про своїх клієнтів. Так як головним продуктом компанії є дзвінок до іншого абонента, користувачі виконують сотні тисяч операцій в день. Запис деталізації дзвінків зберігається в базі даних, яка стає непомірно величезною. Телекомунікаційні компанії зберігають дані про своїх клієнтів для їх опису та аналізу, а також дані про мережі, для спостереження стану її складових елементів. Зібрана інформація може бути впорядкована за допомогою інструментів аналізу [5].

Переваги використання CRM в системах телекомунікацій беззаперечні. По-перше, за рахунок єдиної бази з інтелектуально зрозумілим інтерфейсом, знижується кількість необхідних дій для пошуку та аналізу потрібної інформації, що стосується абонентів і пропонованих продуктів. Це значно знижує час обслуговування, а також забезпечує доступ до інформації про користувачів в режимі реального часу. По-друге, збільшується ефективність виконання рутинних завдань, оскільки для прийняття рішень в сферах підтримки знадобляться додаткові

відомості з інших відділів компанії. Використовуючи CRM, оператори можуть швидко вирішити до 80% завдань, поки абонент чекає на лінії. Централізоване зберігання інформації про клієнта і наскрізна ідентифікація незалежно від каналу передачі даних, покращують злагодженість і правильний порядок дій у взаємодії з клієнтом в будь-який час і з використанням різних засобів зв'язку, що здатне збільшити рівень задоволеності абонентів [6].

Надалі обсяг інформації буде рости дуже швидкими темпами, тому кожній компанії потрібні автоматизовані інструменти для трансформації даних в корисну інформацію і знання, що формують інформаційну базу для прийняття ефективних управлінських рішень.

Література:

1. D. Camilovic, Data mining and CRM in telecommunications // Serbian Journal of management, – № 4, 2007. – С. 19-24.

2. Андреева О.Д., Абрамова А.В. Развитие использования цифрового маркетинга в мировой экономике // Российский внешнеэкономический вестник, 2015. – Т. 2015. – №4. – С. 24-41.

3. Володіна Е.Е, Кухаренко Є.Г, Салютін Т.Ю. Економічні основи функціонування інфокомунікаційної компанії // Економіка і якість систем зв'язку, 2017. - № 4 (6). - С. 3-9.

4. Нікуліна А.І., Кухаренко О.Г. Аналіз лояльності споживачів інфокомунікаційних послуг // Телекомунікації та інформаційні технології, 2014. - Т.1. - № 2. - С. 28-29.

5. Зайцева О.О., Болотинюк І.М. Електронний бізнес: Навчальний посібник. / За наук. ред. Н.В. Морзе. – Івано-Франківськ: «Лілея-НВ» – 2015. – 264 с. [Електронний ресурс] // http://www.dut.edu.ua/ua/lib/1/category/669/view/1658.

6. Лейко А.О. «Метод підвищення ефективності роботи з CRM системою» [Електронний ресурс] // http://tk-its.kpi.ua/. URL: http://tk-its.kpi.ua/sites/default/files/2019-03/Leiko_magistr.pdf.

ТЕЛЕКОМУНІКАЦІЇ ТА МЕДИЦИНА

Грушковський Владислав В'ячеславович
Державний університет телекомунікацій
Інформаційних технологій
м. Київ

Телемедицина та можливості її застосування все частіше згадуються останнім часом в контексті медреформи в Україні та протидії пандемії у цілому світі. Для когось це нове поняття. Та насправді у більшості країн це явище переживає друге народження: віртуальні прийоми в умовах світового локдауна — один з найбезпечніших способів проконсультувати пацієнтів і запобігти поширенню коронавірусу в медзакладах. Що означає це поняття – «Телемедицина», як вона працює у світі та в Україні, які нові можливості відкриває лікарям?

Існує багато тлумачень терміну «Телемедицина». Дослівно це «медицина на відстані», від греч. «tele» – вдалині, далеко. Визначити його чітке розуміння важливо з юридичної та

політичної точок зору для коректного впровадження на практиці.

Телемедицина є досить новим напрямком, що розвивається на перетині декількох областей – медицини, телекомунікації, інформаційних технологій. Ця сфера медичних послуг дозволяє пацієнту і лікарю заощадити час і сили, тому що спілкування відбувається онлайн. Це актуально для жителів мегаполісів, які хочуть стежити за своїм здоров'ям і не сидіти в чергах. Але телемедичні технології — це ще і вихід для людей, які живуть у сільській місцевості, адже висококваліфіковані лікарі працюють у містах. Загалом завдяки ринку телемедицини значно скорочуються витрати на лікування, підвищується якість діагностики і реалізується можливість віддаленого моніторингу стану здоров'я.

А для пацієнтів з хронічними захворюваннями і літніх людей це вкрай важливо. Технологічно такого роду телекомунікація повинна забезпечувати пряму передачу медичної інформації в різних форматах (історія хвороби, дані лабораторних досліджень, рентгенівські знімки та результати КТ, МРТ, УЗД тощо), а також відео конференц-зв'язок в режимі реального часу між медичними установами або лікарем і пацієнтами.

З поширенням смартфонів і вебкамертелемедицина вже давно стала звичною практикою в професійному медичному середовищі України. Вона дає багато додаткових можливостей, яких не було до появи IT технологій та гаджетів. Наприклад, пацієнт може відправити лікарю результати аналізів в месенджері і йому не потрібно їхати, сидіти в черзі, щоб почути, що просто треба здати аналізи повторно через місяць.

Телемедичні IT технології дозволяють лікарям і пацієнтам спілкуватися в режимі реального часу. Сеанси можуть проводитися де завгодно. Пацієнт і фахівець зідзвонюються за допомогою спеціалізованих систем відео- або аудіоконференцзв'язку. При цьому вони можуть не лише бачити і чути один одного, але та обмінюватися текстовими і графічними даними. Наприклад, пацієнт може показати лікарю свій рентгенівський знімок, зроблений під час обстеження в іншому медзакладі, і отримати додаткову думку вузького спеціаліста.

Віддалений моніторинг стану пацієнта часто необхідний для спостереження за літніми людьми, які не в змозі дійти до найближчої поліклініки або не можуть самі про себе піклуватися. Сервіс також може нагадувати про прийом ліків. Крім того, віддалений моніторинг потрібний для контролю

здоров'я пацієнтів, яким необхідні регулярні обстеження, а також для спостереження за станом працівників небезпечних виробництв. Усе це здійснюється за допомогою Інтернету речей (IOT) і аналізу великих даних (BigData). Спеціальні датчики на зразок фітнес-трекерів, які носять багато з нас, аналізують показники здоров'я (рівень цукру в крові, кров'яний тиск і таке інше) і передають отримані дані в спеціальне сховище. Там їх знов аналізують, і в разі потенційної небезпеки пацієнтові та його лікарю подається тривожний сигнал.

За допомогою телемедичних технологій лікарі можуть екстрено консультуватися один з одним. При серйозних випадках медику інколи самому потрібна допомога більш кваліфікованого колеги. Якщо такого немає поруч (наприклад, якщо йдеться про сільські лікарні), то єдиний вихід — це спілкування в режимі телеконсультацій чи консиліумів. Тоді фахівець може надати рекомендації, наприклад, чи потрібна операція пацієнтові. Дуже часто це надзвичайно важливо, особливо в ситуаціях, коли йдеться про хронічні патології, які вимагають негайного втручання.

Прямі трансляції хірургічних операцій, під час яких лікарі можуть ставити питання, також належать до телемедицини. Ця технологія може використовуватися також в режимі «теленаставництва», коли більш досвідчений лікар дистанційно контролює дії колеги-початківця в режимі реального часу.

На сьогодні телемедицина залишається у світі одним з найбільш зростаючих напрямів health бізнесу. У глобальній перспективі вона може поліпшити та стандартизувати якість медичної допомоги.

Використання сучасних телемедичних систем є одним з найперспективніших шляхів реформування вітчизняної системи охорони здоров’я, що дає змогу за порівняно короткий строк і в умовах обмеженого фінансування досягти істотного підвищення ефективності використання коштів, що виділяються на вирішення завдань медичного моніторингу.

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПРОБЛЕМИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Даниленко Даніїл Анатолійович
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Телекомунікації є важливою складовою в соціальної та економічної діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації. Розвиток телекомунікацій повинен здійснюватися

випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу.

У сфері телекомунікацій існують такі проблеми:

- низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг;
- використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;
- наявність великої кількості операторів телекомунікацій, що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Стратегією розвитку телекомунікацій є створення умов для економічного зростання та удосконалення механізмів управління розвитком громади на засадах ефективності, відкритості та прозорості, посилення інвестиційної та інноваційної активності, забезпечення належного функціонування транспортної та комунальної інфраструктури, дотримання високих екологічних стандартів, та внаслідок цього підвищення конкурентоспроможності громади, доступності широкого спектра соціальних послуг та зростання добробуту населення.

Розвиток телекомунікацій повинен здійснюватися за такими основними напрямами:

- прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних;
- сприяння реалізації регуляторної політики у сфері телекомунікацій, спрямованої на об'єднання можливостей

суб'єктів ринку телекомунікацій з метою розв'язання основних проблем сфери, підвищення ефективності їх діяльності;

- удосконалення нормативно-правової бази у сфері телекомунікацій.

Державна підтримка розвитку телекомунікацій

Прискорений розвиток телекомунікацій є одним із основних чинників, що впливатиме на розбудову національної економіки та масове впровадження інформаційних технологій, побудову в Україні інформаційного суспільства, на процес інтеграції України в ЄС та у світову економіку, а також збільшення надходжень до державного бюджету.

Для реалізації завдань Концепції необхідна державна підтримка розвитку телекомунікацій за такими напрямами:

- залучення вітчизняних наукових установ та окремих науковців, спрямування їх діяльності на вирішення системних питань, що впливають на розвиток телекомунікацій;
- розвиток науково-технічної та регуляторної політики у зазначеній сфері шляхом прискореного розроблення рекомендацій, нормативних документів і регламентів, організації пошукових і науково-дослідних робіт з оптимального використання наявних ресурсів з метою підвищення ефективності діяльності суб'єктів ринку телекомунікацій;
- сприяння залученню зовнішніх та внутрішніх інвестицій для розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах;
- сприяння структурним, технічним і технологічним перетворенням у сфері телекомунікацій, підвищенню ефективності регуляторного впливу на ринок телекомунікацій з використанням рекомендацій міжнародних організацій стосовно організаційних, технічних і фінансових аспектів діяльності;
- нормативно-правове забезпечення діяльності у сфері телекомунікацій;
- фінансова підтримка проведення науково-дослідних робіт з питань розвитку і побудови мереж наступного покоління в Україні.

Висновок:

Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи

при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

Література:

І. Малець Львівський державний університет безпеки життєдіяльності РОЛЬ ТА ПРОБЛЕМИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПРИ НАДЗВИЧАЙНИХ СИТУАЦІЯХ розпорядженням Кабінету Міністрів України від 7 червня 2006 р. № 316-р П. П. В О Р О Б І Є Н К О, В. М. Г Р А Н А Т У Р О В, ДЕРЖАВНЕ РЕГУЛЮВАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНОЇ СФЕРИ УКРАЇНИ Борисова Л.Є., аспірантка кафедри економіки підприємства та корпоративного управління Одеської національної академії зв'язку ім. О.С. Попова ПРОБЛЕМИ ПОДАЛЬШОГО РОЗВИТКУ ПІДПРИЄМСТВ ТЕЛЕКОМУНІКАЦІЙ

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Дверняк Яніна Володимирівна
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Роль і проблеми розвитку телекомунікацій:

- Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.
- Стратегія розвитку телекомунікацій спрямована насамперед на розв'язання зазначених проблем, крім того, передбачає здійснення заходів для подальшого забезпечення розвитку телекомунікацій в Україні на базі телекомунікаційних мереж наступного покоління.

<u>У сфері телекомунікацій існують такі проблеми:</u>

- низький рівень забезпечення населення, підприємств, установ і організацій інтерактивними телекомунікаційними послугами;
- нерівномірність забезпечення телекомунікаційними послугами та обмеженість доступу користувачів до загальнодоступних телекомунікаційних послуг (особливо у сільській, гірській місцевості і депресивних регіонах);
- використання на стаціонарних телекомунікаційних мережах морально застарілого та фізично зношеного аналогового обладнання, що стримує розвиток телекомунікацій та негативно впливає на ефективність роботи операторів телекомунікацій;
- наявність великої кількості операторів телекомунікацій (видано майже 700 ліцензій), що призвело до нескоординованості їх дій та відсутності єдиного підходу до вирішення проблемних питань розвитку телекомунікацій;
- неефективне використання можливостей прокладених волоконно-оптичних ліній зв'язку та побудованих стільникових мереж операторами телекомунікацій;
- недостатній регуляторний вплив держави на ринок телекомунікацій;
- недостатнє фінансове та матеріально-технічне забезпечення розроблення наукового підходу до визначення принципів державної політики щодо регуляторного впливу на ринок телекомунікацій.

Прискорений розвиток телекомунікацій є одним із основних чинників, що впливатиме на розбудову національної економіки та масове впровадження інформаційних технологій, побудову в Україні інформаційного суспільства, на процес інтеграції України в ЄС та у світову економіку, а також збільшення надходжень до державного бюджету.

Для реалізації завдань Концепції необхідна державна підтримка розвитку телекомунікацій за такими напрямами;

- залучення вітчизняних наукових установ та окремих науковців до визначення принципів державної політики у сфері телекомунікацій, спрямування їх діяльності на вирішення системних питань, що впливають на розвиток телекомунікацій;
- розвиток науково-технічної та регуляторної політики у зазначеній сфері шляхом прискореного розроблення рекомендацій, нормативних документів і регламентів, організації пошукових і науково-дослідних робіт з оптимального використання наявних ресурсів (фінансових, трудових, матеріальних, частотних, номерних, адресних тощо) з

метою підвищення ефективності діяльності суб'єктів ринку телекомунікацій;

- сприяння залученню зовнішніх та внутрішніх інвестицій для розвитку телекомунікаційних мереж у сільській, гірській місцевості і депресивних регіонах;

Висновок:

- Сфера телекомунікацій особливу відіграє роль в забезпеченні управління економіки України. Створена така інформаційна система, яка дозволяє забезпечити функціональне, організаційне, економічне і соціальне узгодження та досягнення цілей управління телекомунікацій.
- Телекомунікації відіграють важливу інфраструктурну роль у суспільстві, забезпечуючи оперативний обмін і розповсюдження інформації в процесах соціальної і економічної діяльності суспільства. Телекомунікації виконуватимуть роль комунікаційної основи при побудові інформаційного суспільства в Україні. Розвиток телекомунікацій повинен відбуватися випереджаючими темпами, порівняно з розвитком економіки, з тим, щоб не обмежувати економічний та соціальний розвиток суспільства.
- Ці загальні закономірності повинні стати визначальними для розвитку телекомунікацій України на найближчу і більш віддалену перспективу. Телекомунікації повинні зіграти роль каталізатора у прискореному розвитку економіки та соціальної сфери України, оскільки основний ефект діяльності телекомунікацій проявляється не у вигляді доходів, прибутків і відрахувань у держбюджет, а у вигляді злагодженого і оптимізованого функціонування економіки та соціальної сфери країни, а також у вигляді покращення умов життя громадян.

СОЦІАЛЬНІ МЕРЕЖІ ТА ЇХ ВПЛИВ НА СВІДОМІСТЬ ПІДЛІТКІВ

Ковальчук Олена Віталіївна
Державний університет телекомунікацій
Навчально-науковий інститут менеджменту та підприємництва
м. Київ

З появою Інтернету соціальні мережі дуже глибоко увійшли у наше повсякденне життя, а телефони стали продовженням людської руки. Люди «залипають» у них всюди: у громадському транспорті, ресторанах, колективних зустрічах чи розмовах тет-а-тет [4]

Що таке соціальна мережа - сьогодні відомо практично всім, хто хоч якимось чином вважає себе частиною сучасного суспільства із доступом до мережі Інтернет. Але, здається, що в Україні, на відміну від західних держав, поки що недооцінюють наскільки впливовою може бути дана структура у політичному аспекті, виховному та й взагалі соціальному. Так що ж таке соціальна мережа?[1]

Соціальна мережа - соціальна структура, утворена індивідами або організаціями. Вона відображає розмаїті зв'язки між ними через різноманітні соціальні взаємовідносини, починаючи з випадкових знайомств і закінчуючи тісними родинними вузлами. Вперше термін було запропоновано в 1954 році Дж. А. Барнесом. Максимальний розмір соціальних мереж становить близько 150 осіб, а середній – 123.

Говорячи простими словами соціальна мережа - це віртуальне об'єднання людей, де обмінюються певною інформацією, що в широкому сенсі є характеристикою самого поняття «Інтернет». Причини її існування очевидні: сьогодні люди проводять величезну кількість часу за комп'ютером і звикли обмінюватися інформацією одне з одним насамперед в електронному вигляді, адже це, як мінімум, економить час.

У процесі використання соціальних мереж для спілкування у віртуальному просторі, що становить собою комунікаційний компонент, відбувається вплив на наші комунікативні процеси. У процесі спілкування у соціальних мережах створюється особливий простір (віртуальна реальність) з характерним для нього видом спілкування, де виникають нові правила та закони.

Задоволення потреби у спілкуванні, моральній підтримці – найважливіші потреби особистості підліткового віку. Якщо ми не можемо задовільнити їх в реальному житті, то задовольняємо в інтернет-мережі, яка дає можливість «втекти» від проблем, труднощів, що виникли на певному етапі соціалізації. Однак слід розуміти, що, не зважаючи на те, що в інтернет-мережі інколи можна отримати деякі дані анкетного характеру і навіть фото та реальне зображення співрозмовника, вони не дають реалістичного уявлення про нього. Анонімність спілкування в інтернет-мережі сприяє самопрезентації, надаючи людині можливість не просто створювати про себе враження за власним вибором, але й бути тим, ким вона захоче, що нерідко призводить до виникнення девіантної поведінки та агресивності.

Пізнавальний компонент діяльності людини у мережі Інтернет дає можливість пошуку та засвоєння підлітками інформації, яка розміщена на вебсайтах, метою якого є

розширення, поглиблення, уточнення власного уявлення про світ, реальну та віртуальну дійсність.

На відміну від інших засобів інформації, соціальні мережі поєднують у собі друковану, фото- та відеоінформацію. Використовуючи інтернет-мережу для навчання, підліток може сприймати одну й ту ж інформацію такими каналами сприйняття: зоровим, слуховим, оскільки є можливість прочитати, побачити та почути, що суттєво покращує процес засвоєння інформації.

Перебуваючи у віртуальному світі та вивчаючи ту інформацію, яка розміщена у соціальних мережах, кожен із нас формує свою систему цінностей, яка визначає виняткове ставлення до певних дій, вчинків, явищ як віртуального, так і реального життя; визначає нашу поведінку та майбутню соціальну діяльність, що становить собою ціннісний компонент.

Але роздивляючи позитивні сторони використання соціальних мереж у житті сучасної людини не можна забувати і про негативні сторони використання інтернету – шкоди від них не менше аніж користі.

По-перше, соціальні мережі – це своєрідний наркотик. Скільки відсотків молодих людей може реально контролювати час проведений в онлайні та вчасно змусити себе вийти з Інтернету?[3]

По-друге, залежність від мережі може мати шкідливий вплив на психічне здоров'я. **Зловживання цими перевагами сучасності може робити людей більш нещасними та ізольованими від світу.** Соцмережі не лише спричинюють нещастя, але й призводять до розвитку проблем зі психічним здоров'ям, зокрема, викликають тривогу та депресію.[2]

По-третє, наслідком впливу на психіку людини стала мінливість її самооцінки. Як би там не було, люди схильні порівнювати себе з іншими в соцмережах, слідкуючи за їх естетично ідеальними фотографіями в Instagram або статусом стосунків у Facebook. А це своєю чергою може значно посилити невпевненість у собі.

Четвертим фактором впливу соцмереж на людину є сон. Сон – один із найголовніших аспектів здорового життя. Але більшість з нас звикла користуватися телефоном перед сном, що ускладнює процес засинання. *Переживання тривоги або заздрості від того, що ми бачимо в соцмережах, тримає наш мозок у стані високої бойової готовності, заважаючи заснути. До того ж, світло екранів може придушувати вивільнення мелатоніну, гормону, що допомагає нам почувати себе замореними*.

Можна до безкінечності перераховувати позитивні і негативні аспекти впливу соціальних мереж на життя людини, однак ясно одне - вони стали невід'ємною частиною сучасності, але при правильному використанні і дотримань правил можна уникнути багатьох проблем. Адже навіть незначні зміни можуть принести багато користі.

Література:

1. *https://naurok.com.ua/vpliv-socialnih-merezh-na-formuvannya-osobistosti-pidlitkiv-165291.html*
2. *https://www.bbc.com/ukrainian/vert-fut-42693578*
3. *https://vipsoft.blob.core.windows.net/contest/041cf057f5dfb5204385e35b82eed715.pdf*
4. *https://hromadske.ua/posts/5-prychyn-chomu-sotsmerezhi-staiut-nebezpechnymy*

АНАЛІЗ СОЦІАЛЬНИХ МЕРЕЖ НА ПРЕДМЕТ ВИЯВЛЕННЯ ПОЗИТИВНОГО ЧИ НЕГАТИВНОГО ВПЛИВУ НА КОРИСТУВАЧІВ

Козачук Ярослав Васильович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

У статті розкрито позитивний та негативний вплив всесвітніх та українських соціальних мереж на соціальне та психологічне здоров'я користувачів. В результаті роботи досліджено та проведено теоретичний аналіз такого явища, як соціальні мережі та їх вплив на користувачів. Доведено , що соціальні мережі мають як свої позитивні сторони, так і негативні. Висновки зроблені на основі результатів анкетування людей різних вікових категорій, проведеного в мережі інтернет. В результаті дослідження виявлено найпоширеніший засіб боротьби з залежністю в наш час- блокування освітніми та офісними установами доступу до соціальних мереж.

***Ключові слова**: Соціальні мережі, Facebook, Twitter, instagram, вплив соціальних мереж, користь, негативний вплив,користувачі, обмін повідомленнями.*

Історія існування корпорацій у західному світі охоплює вже п'ять століть, за цей час вони домоглися колосальних успіхів у виробництві матеріальних статків, однак у ролі творців соціального ландшафту корпорації виступають лише одне сторіччя.

Багато соціологів називають XXI століття століттям організацій, і тим не менш питанням про те, що керує внутрішнім життям організації, дослідники стали займатися тільки із середини минулого століття. Так виник новий напрямок в соціології – соціальні мережі. Все це зумовлює актуальність теми нашого дослідження аналізу соціальних мереж.

Чому ми так любимо, проводити час за комп'ютером і в соціальних мережах, як це на нас впливає, чи зможемо ми

сказати собі стоп? (чи зможемо ми зупинитися?) Це і багато іншого я спробував з'ясувати у своїй роботі, а саме: виявити які саме проблеми пов'язані з використанням соціальних мереж, вивчити вплив соціальних мереж на фізичне і психологічне здоров'я людини, вивчити проблему мережевої залежності, провести соціологічне дослідження з проблеми впливу соціальних мереж на учнів.

Поняття «соціальна мережа». Останнім часом соціальні мережі отримали велике поширення як на заході, так і у нас в Україні. Інвестиції в подібні проекти досягають сотень мільйонів і навіть мільярдів доларів. В Україні ці суми перевалили за кілька десятків мільйонів доларів і продовжують зростати, що свідчить про зростаючу популярність і впевненість інвесторів не просто повернення своїх інвестицій, але і їх примноження. Результати численних досліджень свідчать, що соціальними мережами вже охоплено більше половини всіх користувачів Інтернету. В Україні цей показник поки менше світового, але він стрімко зростає.

Соціальні мережі - це співтовариства по інтересах [5]. І з деяких пір, соціальні мережі стали достатньо модним явищем, і як по помаху чарівної палички, в них спрямувалися інтернет-користувачі, як ті що намагаються поспілкуватися, розширити коло своїх інтересів, так і ті, що створюють ці мережі, і що заробляють на них гроші.

Історія виникнення соціальних мереж. Термін « Соціальна мережа » був введений задовго до появи Інтернету і власне сучасних інтернет-мереж, ще в 1954 році соціологом з «Манчестерської школи» Джеймсом Барнсом. Сучасне поняття в простому вигляді означає певний коло знайомих людини, де є сама людина — центр соціальної мережі, його знайомі — гілки цієї соціальної мережі і відносини між цими людьми. Якщо розглядати соціальну мережу більш глибоко, можна виявити, що зв’язки діляться за типами: односторонні і двосторонні; мережі друзів, колег, однокласників, однокурсників і т.д. Першими комп’ютерними соціальними мережами стали, як не дивно, все ті ж групи людей, що використали для створення і підтримання соціальних зв’язків засоби комп’ютерного спілкування, якими стала електронна пошта. Сталося це 2 жовтня 1971 року — день першого повідомлення, надісланого на віддалений комп’ютер, а першими користувачами соціальної мережі стали військові в мережі ARPA Net. Це був перший крок до створення Інтернету і сучасних соціальних інтернет-мереж. З винаходу комп’ютерів, електронної пошти, IRC і багатьох інших 7 серпня 1991 року витекло винахід Інтернету. Саме в цей день британський вчений

Тім Бернерс-Лі вперше опублікував перші інтернет-сторінки і зробив тим самим наступний крок до сучасних соціальних мереж.

Facebook. Найпопулярніша соціальна мережа Facebook , що була створена 4 лютого 2004 року як мережа для студентів. Заступником та головою сервісу є Марк Цукерберг. Головний офіс розташований у місті Менло-Парк, штат Каліфорнія, США. Основною статтею доходу є реклама. Користувачі мають можливість створювати профілі з фотографіями, списками інтересів, контактними даними та іншою особистою інформацією. Вони можуть спілкуватися із друзями та іншими користувачами за допомогою приватних або загальнодоступних повідомлень і чату. Також користувачі можуть створювати і приєднуватися до груп за інтересами та «сторінок уподобань». Деякі з цих сторінок підтримують організації як засоби реклами. Для більшої безпеки Facebook надає своїм користувачам можливість вибирати власні налаштування приватності та осіб, які можуть переглядати окремі частини їхнього профілю. Доступ до веб-сайту безкоштовний. За умовами ім'я користувача та його зображення для профілю (за наявності) будуть загальнодоступними. Налаштування приватності дають змогу користувачам контролювати, хто може бачити інформацію, якою вони діляться, а також хто може знаходити їх у пошуку [2].

Twitter. Соціальна мережа Twitter яка є мережею мікроблогів, що дає змогу користувачам надсилати короткі текстові повідомлення до 140 символів. Створений Джеком Дорсі в 2006 році. Головний офіс знаходиться в Сан-Франциско, штат Каліфорнія, США. Користувач посилає короткий текст, в якому, як правило, повідомляє всім, що він робить, що відбувається в даний момент або повідомляє про новини. Ті зареєстровані користувачі, кому ви цікаві, мають можливість підписатися на розсилку повідомлень від вас і бачити їх завжди у своїй стрічці. Таке спілкування відбувається в реальному часі. Крім того, в Твіттері можна використовувати і особисті повідомлення, які не будуть видні іншим користувачам. Але особливість полягає в тому, що ви можете відправити особисте повідомлення лише тому, хто «стежить» за вами.

Instagram - друга найбільша соціальна мережа у Європі після Facebook.

Соціальна мережа, що базується на обміні фотографіями, дозволяє користувачам робити фотографії, застосовувати до них фільтри, а також поширювати їх через свій сервіс і низку інших

соціальних мереж. Є одним із найпопулярніших сервісів у мистецтві айфонографії. Instagram робить фотографії у квадратній формі — як камери Kodak Instamatic і Polaroid. Більшість же мобільних фоторедакторів використовує співвідношення сторін 3:2. Розробили Instagram Кевін Систром та Майк Крігер, які обидва із Сан-Франциско, вирішивши переорієнтувати свій проєкт Burbn на мобільні фотографії. Застосунок з'явився в магазині App Store компанії Apple 6 жовтня 2010. У січні 2011 року в застосунок були додані хештеги для того, щоб було легше знаходити користувачів і фотографії. До грудня 2010 року в Instagram був один мільйон зареєстрованих користувачів.В липні 2012 року Instagram оголосив про 100 мільйонів завантажених фотографій, в серпні це число досягло 150 млн.Станом на вересень 2017 року сервіс нараховує 800 млн користувачів, з них 500 млн відвідують свої акаунти щодня[1]. У червні 2018 року аудиторія Instagram досягла 1 млрд користувачів.

В Контакті - ВКонтакті почала працювати 10 жовтня 2006 року. Сайт спочатку позиціонував себе як соціальна мережа студентів і випускників елітних російських вищих навчальних закладів, пізніше — як універсальний засіб зв'язку для всіх соціальних груп і віків. У січні 2009 року «В Контакті» вперше обігнав за відвідуваністю на пострадянському просторі свого головного конкурента — «Одноклассники». Соціальна мережа «В Контакті» стала зручним ресурсом для зберігання аудіо та відео записів, де зараз зберігаються мільйони пісень, кліпів, фільмів та іншого контенту.

Одноклассники. Соціальна мережа «Одноклассники» та один з найбільш відвідуваних сайтів російськомовного сектору. Проект був запущений у березні 2006 року. Творець сайту - Попков Альберт Михайлович. Одноклассники - це спеціалізований проект по пошуку друзів шкільних і студентських років. Тут кожен має шанс знайти і відновити втрачені багато років тому дружні і приятельські зв'язки. Сайт об'єднує старих друзів в одну велику мережу яка дозволяє не лише здійснювати пошук людей, але і спілкуватися з ними прямо на сайті, призначати реальні зустрічі.

Українські соціальні мережі. Серед соціальних мереж є також і українські. На початку 2014 року з`явилася одна з наймолодших, найскандальніших, найперспективніших та друга за чисельністю українська соціальна мережа – це WeUA. Ідея створення належить Богдану Оліярчуку, який зібрав команду з 15 талановитих програмістів. Після запуску 1 квітня 2014 року

сайт пережив потужні DdoS-атаки, була навіть введена реєстрація за запрошеннями. Основними недоліками соціальних мереж є їх непопулярність серед багатьох користувачів інтернету. Також немає жодної соціальної мережі, яка б містила б у собі всі потрібні функції.Отже, українські соціальні мережі існують, це не міф, їх вибір досить великий, але варто відзначити, що на даний час всі вони поступаються таким гігантам як: Facebook, Twitter, Instagram, Вконтакті, Одноклассники. **Користь соціальних мереж.**

Зручний обмін інформацією. За допомогою соціальних мереж багато людей обмінюють потрібною їм інформацією. Кожен користувач може не тільки написати текстове повідомлення, а й прикріпити до нього документ, фото, відео, аудіо. Завдяки цьому люди багато дізнаються одне про одного.

Час на зважені дії. В соціальних мережах абсолютно не обов'язково миттєво відповідати на повідомлення. І в цьому безумовно є плюси: розлютившись або засмутившись – людина спочатку подумає, перш ніж так само злісно написати у відповідь. Можливо через пару секунд прийде повідомлення з поясненнями або вибаченнями, і образи вирішені. А в реальному житті вже міг би вийти справжній конфлікт.

Розширені комунікації. Завдяки соціальним мережам люди, що знаходяться один від одного на далекій відстані, отримують можливість спілкуватися. Крім того, в соціальних мережах можна завести нові знайомства, які можуть обернутися справжньою дружбою в реальному житті [6].

Маркетинг та реклама. Оскільки соціальні мережі є засобом для поширення інформації, то з легкістю можна розмістити рекламу на сторінках користувачів, спільнот.

Середовище для розвитку бізнесу. Соціальні мережі - це сьогодні модно, трендово та у всіх на слуху. Користувачі в них днюють і ночують, а там, де з'являється користувач, варто очікувати і на появу бізнесу. Власне, він вже там: про це сигналізує поява вакансій SMM-менеджерів, профільних конференцій, кейсів, заточених під соцмережі, "цифрових" агенцій тощо. За великим рахунком з'явилася ціла бізнес-ніша, але десь там на її тлі досі не вщухають, а після нещодавнього IPO Facebook навіть посилюються, розмови про те, що соціальні мережі - це чергова бульбашка. Так це чи ні, покаже найближчий час.

Користь для освіти. Соціальні мережі сприяють розвитку електронного навчання і освіти в цілому, пропонуючи нові технічні та методичні засоби. Студенти з усього світу можуть підписатися на он-лайн уроки абсолютно безкоштовно і

проходити курс навчання в зручному для себе темпі. Крім лекцій, студенти можуть підтримувати зв'язок з викладачем або брати участь у дискусіях. Дійсно, за останні роки дуже змінилися способи і форми комунікації людей в Інтернеті, адже цим сайтам вдалося технічно реалізувати те, чого потребує сучасна людина, а саме, загальнодоступні соціальні інструменти та засоби взаємодії для побудови свого особистого навчального або робочого простору. У зв'язку з вивченням можливостей використання соціальних мереж в освіті, на заході стає актуальною теорія соціального навчання, яка полягає у припущенні, що люди вчаться найбільш ефективно, коли вони взаємодіють з іншими учнями в рамках якоїсь теми або предмета. Студенти, які навчаються в групах хоча б раз на тиждень, виявляються краще підготовленими, ніж студенти, які займаються самостійно [1]. У соціальному навчанні фокус уваги викладачів повинен зсуватися від вмісту предмета в навчальній діяльності до взаємодії людей, навколо яких цей вміст і знаходиться.

Шкода соціальних мереж .Марна трата часу. Часом ми навіть не замислюємося, скільки часу втрачаємо в соціальних мережах. «Ось тільки на хвилиночку, перевірю нові повідомлення й відразу вийду», а насправді ми часто проводимо в «Facebook», «Однокласниках» або «Вконтакте» цілий вільний вечір і половину робочого дня. Виховання комплексу неповноцінності. Користувачам подобається стежити за життям інших людей, безуспішно заздрячи і страждаючи. Нове фото з відпустки чи чергова нагорода в професійній області колеги або знайомого не можуть не торкнутися нашого самолюбства. Рано чи пізно ми починаємо ставити собі запитання «чому не я?», на яке не можемо знайти відповіді. Це нестримне почуття «аутсайдерства» з кожним днем поглинає людину і заважає рухатися вперед.

Розсіювання уваги. Користувачі люблять перечитувати новинну стрічку, перескакуючи від фотографій з котиками до кримінальних новин або чергового конкурсу. Не проходить і 5 хвилин, як вони забувають, що хотіли зробити і що шукали. У підсумку проходить чимало часу, щоб знову налаштуватися на робочий лад і сконцентруватися на поточному завданні. Людина стає розсіяною як в роботі, так і повсякденному житті.

Непристойні матеріали. На сторінках соціальних мереж розміщено багато матеріалів, які пропагують насильство, педофілію та мають порнографічний зміст.

Ефект «затягування» . Соціальні мережі володіють великим адаптивним потенціалом, тобто, значним ризиком

виникнення залежності. Для цього існує кілька причин. Перша причина полягає в тому, що робота в соціальних мережах дратує центри задоволення в нашому мозку. Ми відчуваємо приємні емоції, кожен раз, коли читаємо доброзичливий коментар під своєю фотографією, отримуємо «лайк», коли хтось залишає позитивний відгук і т. д. Бажання повторного отримання цих емоцій несе нас знову на простори соціальних мереж, змушуючи там проводити все більше і більше часу. "Замість службових обов'язків, співробітники витрачають свій час на "пошуки друзів" і перегляд нових повідомлень, що в свою чергу негативно впливає не тільки на продуктивність працівника, але і на психологічний стан людини. Розриваючись між роботою і віртуальним спілкуванням, у людей виникає стресовий стан, який в свою чергу позначається і на фізичному здоров'ї, - говорить психолог в інтерв'ю [4]. В основі інтернет-залежності, вважають фахівці, лежить насамперед нелюбов і невпевненість в собі. Люди, що страждають "комплексом недостатності", незадоволені своєю зовнішністю або малим увагою оточуючих до своєї персони, найчастіше і підсаджуються на "онлайнову" голку. Як правило, це люди гуманітарного складу розуму, схильні до фантазій, люблячі прибрехати "для краси" і часто видають бажане за дійсність. Справа в тому, що часте відвідування мережі створює в мозку підвищений рівень допаміну - речовини, подібного адреналіну. Залежний відчуває під час спілкування в чатах збудження, яке схоже азартній лихоманці гравця або сексуальному збудженню. Він хоче повторити цей стан і починає використовувати Інтернет як засіб для отримання задоволення.

Спам, шкідливі коди та віруси. На просторах соціальних мереж знаходиться чимало вірусної реклами та спаму. Деякі з них можуть призвести до непоправних наслідків. При вчасно непоміченому вірусі можуть бути пошкоджені файли та порушені параметри операційної системи.

Доступ до приватної інформації .У соціальних мережах є люди з різними намірами. Це як відбиток усього, що бачимо щодня у реальному світі. Не бракує там і кримінальності, потаємних шпигунів, які теж можуть написати про себе неправдиву інформацію у профілі чи замаскуватися під знайому нам людину.

Шкода для здоров’я. Надмірне захоплення соціальними мережами в інтернеті може шкодити здоров'ю через скорочення спілкування з реальними людьми. На думку вчених, брак спілкування може негативно впливати на роботу імунної системи організму, гормональний баланс, роботу артерій і

процеси мислення, що в довгостроковій перспективі підвищує ризик появи і розвитку таких хвороб, як рак, серцево-судинні захворювання і недоумство.

Вплив соціальних мереж на підлітків. Сучасний світ диктує свої правила. Неодмінними атрибутами, без яких неможливо обійтися, є комп'ютери та мобільні телефони.Саме підлітки швидше будь-якого дорослого вміють правильно визначити необхідність знань сучасних технологій та їх користь. Але з появою соціальних мереж, з'явилася додаткова складність у спілкуванні з дітьми.Мода на соціальні мережі торкнулася, перш за все, підростаючого покоління. Підліток живе окремим життям всередині комп'ютера: шукає нових друзів для спілкування, нові захоплення, любов. Це позбавляє дитину-підлітка від давить почуття самотності.Підліток ідентифікує себе, вступаючи в різні групи і спільноти. Він приміряє на себе різні ролі і вирішує, що саме підходить йому.Існує і зворотний бік такого спілкування — відхід від справжнього життя, неможливість налагодити контакти з реальними людьми. І ця проблема дійсно дуже небезпечна: підліток замикається на своїх переживаннях, перестає спілкуватися з рідними і близькими, так як не знаходить належного розуміння. Підлітки втрачають навик прояву інтересу до інших людей.Особливо соціальні мережі, на погляд вчених, небезпечні для підлітків, так як формують у них помилкове враження, що любов і дружбу легко завоювати і так же легко зруйнувати. Крім того, на думку доктора Хіманшу, людям, звиклим до швидкого перебігу інтернет-життя, реальність може здатися занадто нудним, і вони можуть спробувати "оживити" її, здійснюючи імпульсивні вчинки, в тому числі спроби самогубства, оскільки їм властиво занижувати цінності реального життя[4].

СОЦІАЛЬНІ ДОСЛІДЖЕННЯ

Найпопулярніші соціальні мережі в Україні

Згідно Statista.com, станом на березень 2019 року найбільш популярною соціальною мережею в Україні був Facebook, яким регулярно користуються 44 відсотки учасників опитування. Instagram посів друге місце з часткою 18 відсотків, а 13% респондентів взагалі не користувалися соціальними мережами. 19 мільйонів українців є користувачами Facebook. Другу сходинку посів I*nstagram* — більше 12 мільйонів акантів , ВКонтакті -7 мільйонів українських акаунтів, Однокласники -4 мільйона акаунтів, а в Twitter близько 0,5 мільйона твіттер-акаунтів.

Мною було проведено дослідження учнів 8-их, 10-их та 11-их класів БНВО «Ліцей – МАН»,одного з навчальних

закладів м.Білої Церкви . В дослідженні взяло участь 27 учнів 8-их класів, 17 учнів 10-ого класу та 25 учнів 11-их класів. А також для порівняння в анкетуванні взяли участь дорослі. Була складена анкета, за допомогою якої я отримав відповіді на питання стосовно реєстрації та відвідування соціальних мереж. Було отримано такі результати: виявилось, що 26% 8 класу, 59% 10 класу, 32% 11 класу, 64% дорослих відвідують соціальні мережі щодня.

На питання: скільки часу ви проводите в соціальних мережах, отримали такі результати: 30% 8 класу, 76% 10 класу, 44% 11 класу, 55% дорослих проводять в соціальних мережах кілька годин на день. Але, незважаючи на це, лише 22% 8 класу, 6% 10 класу, 32% 11 класу та 27% дорослих визнають, що відчувають залежність від соціальних мереж. В результаті проведених опитувань і обробки інформації, можна виділити шляхи вирішення проблем, пов'язаних з використанням соціальних мереж:

1. Обмеження часу перебування в мережі.

2. Пошук альтернативних способів проведення часу (наприклад: заняття спортом, малювання, вишивання, читання книг тощо).

3. Надання більшої уваги своєму реальному житті (проблемам в школі, в сім'ї, друзів).

4. Збільшення часу перебування в компанії друзів.

Також було проведено опитування за допомогою програми Survey Monkey на тему ставлення молоді до соціальних мереж та спілкування в них. З опитування можна зробити висновок, що близько 94% молоді зареєстровані в соціальній мережі I*nstagram* а також лише 1,5% - не зареєстровані в жодній соціальній мережі. Серед респондентів: 62% - жінки від 16 до 20 років; 20% - чоловіки від 16 до 20 років; 18% - старші люди. Третина респондентів нейтрально ставляться до знайомств в соціальних мережах, відповідно вважаючи це користю. Близько 40% користувачів задоволені кількістю наявних соціальних мереж.33% користувачів зареєстровані в соціальній мережі близько п’яти років. Близько половини відповіли, що користуються соціальними мережами для полегшення спілкування з друзями та заходять на свою сторінку кожного дня. Оскільки соціальні мережі забирають багато часу, то варто було провести дослідження, як вони впливають на спілкування з друзями. У більшості респондентів у друзях є близько 200-300 користувачів, але половина з них спілкуються зазвичай лише з декількома. Що відповідно і впливає на спілкування в реальному світі, оскільки

близько половини спілкуються лише з декількома друзями, але значно шокує той факт, що зустрічаються лише декілька разів на місяць. 16% користувачів користуються онлайн-іграми та додатками, що значно впливають на трату вільного часу.

Серед користувачів інтернету було проведено опитування що до їх думки на рахунок користі та шкоди соціальних мереж. Серед користі більшість респондентів відмітили спілкування, швидкий обмін інформацією та нові знайомства; серед шкоди – залежність, марна трата часу та деградація суспільства.

В результаті проведеного нами теоретичного аналізу такого явища, як соціальні мережі, можна зробити наступні висновки. Соціальні мережі - це комп'ютерні технології, які отримали значне поширення в світі інтернету на сьогоднішній день: більше половини його користувачів зареєстровані в тій чи іншій соціальній мережі. Віртуальні соціальні мережі є полем арени сучасних інформаційних війн і засобом супроводу різних військових і політичних процесів протиборчих сторін. Активне використання соціальних мереж дозволяє оперативно впливати на думку і поведінку людей, що перетворює їх на вогнище битв груп різних інтересів. Масштаби впливу на людей та управління подіями відкриває перед мережами великий спектр вирішуваних завдань. Відсутність цензури і різного роду перешкод дозволяє діяти користувачам мережі на передовій, створюючи сприятливу основу успішним діям у віртуальному та реальному просторі. Все це дозволяє нам сказати про те, що соціальні мережі перетворюються на поле арени інформаційного протиборства. Можливості онлайн-мереж й інших технологій здійснюють значний вплив на організацію мережевих структур, що використовуються прихильниками "кольорових революцій", їхню структурованість і тактику. Соціальні мережі мають як свої позитивні сторони, так і негативні. Одним з негативних наслідків поширення соціальних мереж є формування у людини психологічної залежності від них. Базою для зародження цього стану, на думку фахівців, є невпевненість в собі людини. Надмірне захоплення соціальними мережами, на думку вчених, шкодить як соціальному, так і психологічному здоров'ю. Найбільш небезпечно дане захоплення для підлітків . Найпоширенішим і найвикористовуванішим засобом в боротьбі із залежністю в наш час є блокування освітніми та офісними установами доступу до соціальних мереж.Соціальні мережі можуть стати повноцінною освітнім середовищем, де кожен бажаючий може провести час, не просто переглядаючи стрічки новин і сторінки друзів, а й отримати масу знань у зручний для себе час і в комфортній обстановці.

Література:

1. Webtexts [електронний ресурс]/Користь соціальних мереж - в чому суть. - Изд: Контент-издательство. - Режим доступу:.texts.com.ua/go/ru/article--ResourceID--9529--category--travel--page.html,вільний.

2. Все про соціальні мережі [електронний ресурс]/Велика доповідь про соціальні мережі. - Режим доступу:vseseti.wordpress.com, вільний.

3. Хабрахабр [Електронний ресурс]/Соціальні мережі. Перспективи розвитку і способи монетизації. - Режим доступу: habrahabr.ru/blogs/social_networks/22811/,вільний.

4. Центр інформаційних комунікацій [електронний ресурс]/Спілкування в соціальних мережах шкодить здоров'ю. - Режим доступу:.commcenter.ru/mmedia/articles/2009_02_26_02.html, вільний.

5. Вікепедія [Електронний ресурс]/Соціальні мережі. - Режим доступу:ru.wikipedia.org/, вільний.

6. Соціальні мережі від А до Я [електронний ресурс]/Більше часу на спілкування. - Режим доступу: .social-networking.ru/papers/36/,вільний.

7. Bigness.ru [електронний ресурс]/Соціальні мережі: пожирачі часу або корисні ресурси. - Режим доступу: .bigness.ru/articles/2008-12-09/internet/5373,вільний.

ПОПУЛЯРНІСТЬ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ ПІД ЧАС КАРАНТИНУ

Левандовська Валентина Андріївна
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Розвиток телекомунікаційних систем. Вплив телекомунікацій на повсякденне життя користувачів. Чи були підготовленні компанії до збільшення відсотку користування їх платформою. Інтернет, соціальне життя, на скільки виросла популярність електронних ресурсів. Заходи підприємств для більш ефективного функціонування під час карантинних норм.

Через карантин і перехід багатьох на віддалену роботу, суспільство стало набагато більше користуватись інтернетом. І це – істотно збільшило навантаження на мережі телекомунікаційних операторів.

Крім того, у відомстві наводять дані компанії Huawei про те, як у період карантину найбільш уражені держави - Китай, Італія, Іспанія, Німеччина, Велика Британія, Франція - відчули помітне зростання в обсягах фіксованого трафіку. Зокрема, в Іспанії зафіксовано збільшення трафіку майже на 40%, в Італії – більше 70% при значному зосередженні на онлайн-іграх, у Німеччині – незначне зростання у 16%, у Британії – 20-30% приросту, у Китаї – 70% і більше. «Українська» цифра, наразі, - близько 25% [3].

Різке зростання популярності відеодзвінків і трансляцій, популярність регіональних ЗМІ та повернення від смартфона до комп’ютера.

За час карантину користувачі в США стали частіше виходити в інтернет за допомогою комп’ютерів, ніж мобільних

телефонів, говориться в дослідженні аналітичних компаній SimilarWeb і Apptopia.

Найбільшою популярністю користуються сервіси потокового відео на кшталт Netflix або Youtube, а також соцмережа Facebook. Популярність веб-версій відеосервісів виросла на 16% і 15,3% відповідно. Веб-версія Facebook показала приріст в 27% при 1,1% росту додатку.

Виріс трафік в застосунках для відеодзвінків на кшталт Google Duo і Houseparty і в локальній соцмережі nextdoor.com.

Також приріст аудиторії показали сервіси для віддаленої роботи та навчання. Аудиторія Zoom перевищила 6 млн користувачів, Google Classroom 4 млн. Кількість користувачів Microsoft Teams і Hangouts теж зросла, але не так значно.

Різко зріс трафік у регіональних видань, і у деяких національних ЗМІ. У той же час вірусні ресурси і сайти з фейковий інформацією втратили значну частину інформації.

Також серйозно впала популярність у спортивних ресурсів через масову скасування спортивних заходів. У той же час, зростає трафік у онлайн відео ігор і сервісів, які дозволяють дивитися трансляції кіберспорту. Наприклад, трафік Twitch виріс на 20%. Також продовжує зростати популярність сервісу коротких відео TikTok який і до пандемії був одним з найбільш завантажуваних сервісів [2].

Кількість продажів у інтернет-магазинах. Основним спостереженням є впевнене зрастання кількість. Можливо, ростуть тільки певні категорії, а інші в занепаді, але тенденція очевидна. Зараз загальна кількість замовлень перевищує показники, які були перед карантином.

Netpeak проаналізували сотні інтернет-магазинів і відзначили значний приріст продажів у 12 нішах, до яких відносяться інструменти, обладнання, товари для будинку, саду, будівництва та ремонту. Також в їх числі їжа та напої, побутова техніка, меблі, текстиль, електроніка, а також товари для спорту, відпочинку та хобі. Щоб дізнатися точні показники інтернет-магазинів до і під час карантину,

Світ стрімко змінюється. Щоб залишатися на плаву, бізнеси мають бути гнучкими та постійно впроваджувати актуальні зміни. Наприклад:

- оперативно перевести всю команду на віддалену роботу;
- змістити фокус команди розробки на інтеграцію нових служб доставки та розвиток існуючих інтеграцій;
- почати активно займатися проектами, які раніше відклали б на потім [1].

Вистновок. Завдяки технічній підготовленості компаній та оперативним діям під час карантину користувачі могли легко використовувати інтернет ресурси для роботи, навчання, відпочинку, шопінгу тощо. Саме завдяки розвитку телекомунікаційних мереж користувачі знаходилися дома, не виходячи на вулицю без великої надібності, тим самим оберігаючи себе і навколишній світ.

Література:

*1. «Кількість продажів під час карантину вища, ніж перед 8 березня: тенденції на ринку ecommerce**»;** стаття, Київ, 2020; Електронний ресурс. Режим доступу: https://horoshop.ua/ua/blog/karantin-tendentsii-na-rynke-ecommerce/*

2. «Інтернет на карантині. Як змінилася поведінка користувачів мережі під час пандемії – дослідження»; стаття, Київ, 2020; Електронний ресурс. Режим доступу: https://nv.ua/ukr/biz/tech/zoom-na-kompaniyu-podali-v-sud-cherez-vrazlivostey-v-dodatku-ostanni-novini-50080901.html

3. «Карантин та українські телекомунікації: навантаження посильне, тарифи не виростуть»; стаття, Київ, 2021; Електронний ресурс. Режим доступу: https://www.ukrinform.ua/rubric-technology/2911889-karantin-ta-ukrainski-telekomunikacii-navantazenna-posilne-tarifi-ne-virostut.html

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Палецька Альона Олегівна
Державний університет телекомунікацій
Навчально-наукового інституту Менеджменту і підприємництва
м. Київ

Науково-технічна революція, що сталася у XX столітті, помітно змінила умови та характер економічного розвитку. Швидке розповсюдження в усьому світі наукових відкриттів, технічних винаходів, інформаційних технологій, нових засобів комунікацій – усе це чинить вагомий вплив на економіку, політику та культуру усіх країн світу. Стратегічною метою телекомунікацій є необхідність забезпечення споживачів телекомунікаційними послугами. Розвиток телекомунікацій повинен відповідати зростаючим потребам інформаційного суспільства щодо надання послуг споживачам з урахуванням існуючого економічного та соціального стану України.

Роль і проблеми розвитку телекомунікацій, стратегія розвитку та аспекти телекомунікаційної системи.

Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне передавання інформації. Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняно із загальними темпами розвитку економіки і буде визначальним на найближчу і більш віддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.

Роль телекомунікацій у соціальних відносинах набуває все більшого значення. В останні роки популярність соціальних мереж різко зросла. Такі сайти дозволяють користувачам спілкуватися один з одним, а також розміщувати фотографії, події та заповнювати власний профіль. У профілі можна вказати вік, інтереси та статус відносин. Таким чином, ці сайти можуть відігравати важливу роль у всьому, починаючи від організації соціальних інтересів до міжособових стосунків.

Телекомунікації зіграли значну роль у соціальних відносинах. Тим не менш, такі пристрої, як телефони, спочатку рекламувались з акцентом на практичність (наприклад, можливість ведення бізнесу або замовлення послуг до дому) не звертаючи акцент на соціальну значущість. Лише наприкінці 1920-х і 1930-х років соціальна значущість пристрою стала основною в телефонній рекламі. Нові акції почали звертатися до емоцій споживачів, підкреслюючи важливість соціальних бесід і залишаючись пов'язаними з родиною та друзями.

До соціальних мереж, такі послуги, як служба коротких повідомлень (SMS) та телефонія також мали значний вплив на

соціальну взаємодію. У 2000 році дослідницька організація Ipsos MORI повідомила, що 81 % користувачів віком 15—24 роки використовують СМС для координації соціальних заходів.

Розвиток телекомунікаційної сфери стримується за рахунок низки проблем, які виникають унаслідок науково-технічного прогресу, кризового становища економіки, зниження обсягу інвестування та доходів верств населення тощо.

В умовах телекомунікаційної сфери необхідно виділити виробничий, науково-технічний, організаційно-економічний, соціальний та екологічний аспекти протиріч, які і формують відповідні проблеми. У зв'язку з цим слід розуміти поняття проблеми як концентроване вираження виробничих, науково-технічних, економічних та соціальних протиріч, що носять складний характер і вимагають свого вирішення.

Проведення розбудови телекомунікаційної сфери не може бути здійснено без аналізу проблем і протиріч накопичених і знов виникаючих в старих системах управління. Тому стає таке завдання як створити таку систему управління, яка буде підготовлена до вирішення наявних проблем і протиріч. У роботі не представляється можливим розкрити весь перелік питань, пов'язаних з вирішенням усіх наявних проблем у сфері телекомунікацій.

Для аналізу розглядається лише деякий перелік протиріч, наявних в області задоволення послуг зв'язку, які носять різний характер. До них можна віднести:

- проблему цифрового розриву, яка пов'язана з недостатньо рівномірним розповсюдженням сучасних технологій;
- недоліки тарифної політики, у зв'язку з чим виникають проблеми зі взаєморозрахунками між телекомунікаційними підприємствами та споживачами послуг зв'язку, що спричиняє конфлікти, а, як наслідок, підвищуються тарифи на телекомунікаційні послуги. Крім того, існує проблема із забезпеченістю населення універсальними послугами зв'язку;
- фізичний та моральний знос обладнання, що спричиняє погіршення якості послуг зв'язку;
- недосконаліть стратегії розвитку телекомунікаційної сфери, тобто відсутність єдиної збалансованої стратегії розвитку та планування у телекомунікаційній сфері;
- недосконаліть нормативно-правової та законодавчої бази, немає узгодженості між нормативно-правовим документами, крім того більшість законодавчих документів не відповідають стану як ринкової економіки, так і державної політики;

- складність отримання та використання обчислювальних ресурсів за рахунок їхньої нерозвиненості;

- недостатність кількості висококваліфікованих фахівців та зменшення їхньої кількості у зв'язку з постійною еміграцією, що сприяє зменшенню кількості інноваційних, науково-дослідних та дослідноконструкторських робіт;

- відсутність механізму підтримки вітчизняного виробника, що спричиняє неможливість забезпечити себе продукцією власного виробництва;

- нестабільну економічну і політичну ситуацію в країні, що сприяє збільшенню рівня інфляції та безробіття, зменшенню споживання послуг зв'язку.

Стратегія розвитку телекомунікацій спрямована насамперед на розв'язання зазначених проблем, крім того, передбачає здійснення заходів для подальшого забезпечення розвитку телекомунікацій в Україні на базі телекомунікаційних мереж наступного покоління.

Розвиток телекомунікацій повинен здійснюватися за такими основними напрямами:

- прискорення розвитку телекомунікаційних мереж з використанням новітніх технологічних досягнень (радіотехнологій, волоконно-оптичних, пакетних технологій тощо);

- сприяння реалізації регуляторної політики у сфері телекомунікацій, спрямованої на об'єднанняможливостей суб'єктів ринку телекомунікацій з метою розв'язання основних проблем сфери, підвищення ефективності їх діяльності.

- удосконалення нормативно-правової бази у сфері телекомунікацій.

ВИСНОВКИ

Отже, концепція визначає проблеми розвитку телекомунікацій, стратегію і основні шляхи їх розв'язання, а також принципи забезпечення комплексного розвитку телекомунікацій. Для реалізації завдань передбачається залучити ресурси мереж загального користування різних форм власності, забезпечити взаємодію цих мереж з урахуванням потреб національної безпеки та оборони держави, захист інформації та безпеки критичних елементів мереж, а також управління всіма мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Стратегія розвитку телекомунікаційних мереж повинна базуватися на використанні новітніх технологій, які відповідають міжнародним стандартам, враховувати необхідність технологічної взаємодії всіх мереж

при наданні телекомунікаційних послуг, забезпечити підвищення ефективності їх функціонування.

Література:

1. *https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BB%D0%B5%D0%BA%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0*
2. *https://web.archive.org/web/20170531035748/http://posibnyky.vntu.edu.ua/e_s/index.htm*
3. *http://www.ej.kherson.ua/journal/economic_14/143.pdf*
4. *https://www.kmu.gov.ua/npas/39141641*

ЩО ТАКЕ ТЕЛЕМЕДИЦИНА ТА ЯКІ ІСНУЮТЬ МОЖЛИВОСТІ ЇЇ ЗАСТОСУВАННЯ

Пікож Яна Олександрівна
Державний університет телекомунікацій
Навчально-наукового інституту Менеджменту і підприємництва
м. Київ

Існує багато тлумачень терміну «Телемедицина». Дослівно це «медицина на відстані», від грец. «tele» – вдалині, далеко. У рамках політики Всесвітньої Організації Охорони Здоров'я (ВООЗ) в області телемедицини у 1997 році було запропоновано наступне визначення. Телемедицина – це метод надання послуг з медичного обслуговування там, де відстань є критичним чинником. Послуги здійснюються медичними працівниками з використанням інформаційно-комунікаційних технологій з метою отримання інформації, необхідної для діагностики, лікування і профілактики захворювання.

Телемедицина є досить новим напрямком, що розвивається на перетині декількох областей – медицини, телекомунікації та інформаційних технологій. Ця сфера медичних послуг дозволяє пацієнту і лікарю заощадити час і сили, тому що спілкування відбувається онлайн. Це актуально для жителів мегаполісів, які хочуть стежити за своїм здоров'ям і не сидіти в чергах. А ще це вихід для людей, які живуть у сільській місцевості, адже висококваліфіковані лікарі працюють у містах. Загалом завдяки ринку телемедицини та розвитку телекомунікацій значно скорочуються витрати на лікування, підвищується якість діагностики і реалізується можливість віддаленого моніторингу стану здоров'я.

Технологічно такого роду телекомунікація повинна забезпечувати пряму передачу медичної інформації в різних форматах, а також відео конференц-зв'язок в режимі реального часу між медичними установами або лікарем і пацієнтами.

ТЕЛЕМЕДИЧНІ ПОСЛУГИ

Телемедичні ІТ-технології дозволяють лікарям і пацієнтам спілкуватися в режимі реального часу. Сеанси можуть проводитися де завгодно. Пацієнт і фахівець зідзвонюються за допомогою спеціалізованих систем відео- або аудіоконференцзв'язку. При цьому вони можуть не лише бачити і чути один одного, але й обмінюватися текстовими і графічними даними. Наприклад, пацієнт може показати лікарю свій рентгенівський знімок, зроблений під час обстеження в іншому медзакладі, і отримати додаткову думку вузького спеціаліста.

Віддалений моніторинг стану пацієнта часто необхідний для спостереження за літніми людьми, які не в змозі дійти до найближчої поліклініки або не можуть самі про себе піклуватися. Сервіс також може нагадувати про прийом ліків. Крім того, віддалений моніторинг потрібний для контролю здоров'я пацієнтів, яким необхідні регулярні обстеження, а також для спостереження за станом працівників небезпечних виробництв. Усе це здійснюється за допомогою Інтернету речей (IOT) і аналізу великих даних (Big Data). Спеціальні датчики на зразок фітнес-трекерів, які носять багато з нас, аналізують показники здоров'я (рівень цукру в крові, кров'яний тиск і таке інше) і передають отримані дані в спеціальне сховище. Там їх знов аналізують, і в разі потенційної небезпеки пацієнтові та його лікарю подається тривожний сигнал.

За допомогою телемедичних технологій лікарі можуть екстренно консультуватися один з одним. При серйозних випадках медику інколи самому потрібна допомога більш кваліфікованого колеги. Якщо такого немає поруч, то єдиний вихід — це спілкування в режимі телеконсультацій чи консиліумів. Тоді фахівець може надати рекомендації. Дуже часто це надзвичайно важливо, особливо в ситуаціях, коли йдеться про хронічні патології, які вимагають негайного втручання.

Розвиваються й мобільні телемедичні комплекси (переносні, на базі реанімобіля тощо) для роботи на місцях аварій. Малогабаритні мобільні діагностичні комплекси використовуються у відсутності телемедичних кабінетів і центрів, безпосередньо там, де виникла необхідність: у машинах швидкої допомоги, віддалених лікарнях, бригадах медицини катастроф і санітарної авіації, медичних формуваннях відомств з надзвичайних ситуацій та оборони.

Звичайно, можливості телемедицини є обмеженими – ніхто операцію таким чином робити не буде. Адже не можна, наприклад, послухати серце, зробити повноцінну кардіограму. Але у певних ситуаціях телемедицина може врятувати життя.

Красномовним прикладом цього є застосування відеоконсультацій під час пандемії коронавірусу.

МАЙБУТНЄ РИНКУ ТЕЛЕМЕДИЦИНИ

На сьогодні телемедицина залишається у світі одним з найбільш зростаючих напрямів бізнесу у сфері здоров'я. У глобальній перспективі вона може поліпшити та стандартизувати якість медичної допомоги. Аналітики оцінюють темпи зростання телемедичних сервісів на рівні 18-20% щорік протягом наступних п'яти років.

За результатами досліджень американських компаній, глобальний ринок телемедицини у 2019 році складав $40 млрд. І це дані, відомі до початку пандемії. Компанія Teladoc – лідер телемедичного сервісу консультацій у США, у 2018 році заробила близько $1 млрд. І ще на той час за оцінками маркетологів це був лише 1% можливостей.

Крім того, вірогідне переорієнтування розподілу коштів системами охорони здоров'я країн. Так, представники охорони здоров'я Великобританії зазначають, що 80% всіх очних консультацій можна проводити заочно. А заощаджені кошти направити на розробку медичних приладів, програмного забезпечення мобільних застосувань і сервісів.

Тож на світовому ринку телемедицини варто чекати нових проривів, глобальних переформатувань систем охорони здоров'я, у кожній країні на свій кшталт, які відіб'ються на роботі медзакладів та лікарів. Попри складні виклики через пандемію у світі, саме зараз завдяки телемедицині у сфери охорони здоров'я є можливості оновитися і стати ще ближче до пацієнтів. Дуже важливо цей шанс не прогавити.

ВИСНОВКИ

Отже, можемо сміливо сказати, що телекомунікації здійснюють вплив на соціальну сферу життя людини. Вони вже навіть допомагають у лікуванні, діагностуванні хвороб, коротше кажучи - у медицині. І ця тенденція буде тільки зростати з роками, тому що телемедицина на сьогоднішній день знаходиться на самому початку шляху свого розвитку. Але, незважаючи на те, що цей напрямок є відносно новим, він уже здобув свою популярність та довів свою дійсність та корисність.

Література:

1. *medinet.com.ua*
2. *wikipedia.org*
3. *moz.gov.ua*
4. *who.int*

РЕЧЕЙ

Поліщук Андрій Русланович
Державний університет телекомунікацій
Навчально-науковий інститут Інформаційних технологій
м. Київ

Перехід до четвертої промислової революції характеризується конвергенцією передових технологій і стиранням межі між об'єктами фізичної, цифровий і біологічних сфер. Ґрунтуючись на досвіді попередніх промислових революцій, очікується стрімке зростання інноваційних технологій, що впливають на розвиток різноманітних сфер суспільного життя. До числа таких технологій відноситься Інтернет речей, все більше затребуваний бізнес-спільнотою та постійно нарощує свій ринковий потенціал.

На основі аналізу різних практик (Gartner, IDC, McKinsey, Forrester, IoT Analytics і т.д.) була складена авторська класифікація ринку Інтернету речей, в основі якої в якості критерію обраний суб'єкт ринку Інтернету речей - бізнес (промисловий Інтернет речей), споживачі (споживчий сегмент Інтернету речей), держава (державний сегмент Інтернету речей).

Промисловий Інтернет речей перетворює бізнес-процеси, підвищує ефективність всього ланцюжка створення вартості, що в кінцевому рахунку призводить до формування нових бізнес-моделей і ринків. Основними напрямками застосування технологій Інтернету речей є ефективне управління поставками, вантажними перевезеннями і активами, діагностика і телеметрія машин, управління запасами, контроль промислової автоматизації, моніторинг обладнання в реальному часі та ін.

Використання технологій Інтернету речей дозволяє вивести виробництво на якісно новий рівень. В результаті стає можливим інтегрувати в виробництво гнучкі промислові системи, а також цифрові системи управління, що спрощує управління виробництвом та прискорює його. У зв'язку з цим необхідно своєчасно впроваджувати перспективні технології, однак через високу вартість ноу-хау впровадження інновацій стає скрутним, хоча і є ключовим питанням. Також важливо приділяти достатню увагу компетентності співробітників і вдосконалювати їх навички.

Інтернет Речей в споживчому сегменті сприяє поліпшенню якості життя за рахунок автоматизації багатьох повсякденних операцій, звільнення часу і надання нових можливостей, раніше недоступних для споживачів.

Технології «розумного» будинку спрямовані на забезпечення максимально комфортного розміщення, безпеки та ресурсозбереження. Вона включає наступні напрямки: управління освітленням, безпеку і контроль доступу, управління системами опалення, вентиляції і кондиціонування, ІКТ системи

в області розваги, медична допомога на дому, а також «розумна» кухня.

Технології Інтернету речей можуть використовуватись у сфері комунальних послуг, і їх використання дозволяє знизити витрати на електроенергію, водовідведення та опалення в рамках домашнього господарство. Така економія ресурсів надає позитивний вплив на навколишнє середовище через скорочення кількості споживаних природних ресурсів, в тому числі невідновлюваних.

Ще однією перевагою від використання технологій Інтернету речей в області житлово-комунального господарства є економія часу на оформлення документів (заповнення квитанцій, збір інформації про щомісячні витратах на воду і електроенергію). Рішення проблеми збору даних для повторюваних рутинних транзакцій можливо завдяки створенню «розумних» лічильників (лічильники води, електроенергії, тепла), підключених до системи Інтернету речей і здатних відправляти повідомлення про оплату на смартфон.

У свою чергу, технології Інтернету речей в міському середовищі спрямовані на розробку інноваційних рішень для інфраструктури, енергозбереження, будівництва та організації суспільного простору. Підключення встановлених датчиків на транспортних засобах і дорогах дозволяє контролювати рух в реальному часу. Крім того, розвиток подібної міської інфраструктури збільшує ймовірність виявлення викрадених автомобілів.

Висновок

Слід зазначити, що частина населення не помічає, як технології Інтернету речей поступового, але стають частиною їх повсякденного життя. Вжезараз, набуваючи нові апартаменти, споживачі часто отримують нове житло з вбудованими рішеннями Інтернету речей, спрямованими на економію споживаної електроенергії і води. Необхідно інформувати населення про нові можливостях, що виникають в результаті використання пристроїв Інтернету речей для стимулювання попиту на них з боку як бізнесу, так і населення. Також необхідно відзначити, що технологія Інтернету речей, будучи однією з ключових технологій четвертої промислової революції, аналогічно попереднім промисловим революціям впливає на ринок праці. З одного боку, зростає попит на висококваліфікованих фахівців, особливо в області хмарних обчислень, великих даних і т.д. Але, з іншого боку, поширення Інтернету речей призводить до зниження попиту на низько кваліфіковануробочу силу. Для вирішення виникаючих

соціальних проблем необхідно реалізовувати програми з підвищення кваліфікації співробітників як на державному рівні, так і на мікрорівні (рівні підприємств).

Література:

1. Enterprise Architecture Management for the Internet of Things: https://www.researchgate.net/publication/278031195_Enterprise_Architecture_Management_for_the_Internet_of_Things

2. The expanding and changing impact of IoT data on IT infrastructure:https://www.i-scoop.eu/internet-of-things-guide/iot-it-infrastructure/

3. Влияние технологий Интернета вещей на экономику: https://cyberleninka.ru/article/n/vliyanie-tehnologiy-interneta-veschey-na-ekonomiku/viewer

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Притиковський Ростислав Миколайович
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

У ст. 3 ЗУ «Про телекомунікації» зазначено, що вони є невід'ємною частиною виробничої та соціальної інфраструктури України і призначені для задоволення потреб фізичних та юридичних осіб, органів державної влади в телекомунікаційних послугах [1], а ст. 6 називає останнє одним з основних принципів діяльності у цій сфері. Телекомунікації відіграють важливу роль у розвитку економіки та у створенні належних умов життєдіяльності населення, адже забезпечують обмін інформацією у різних питаннях. Попит споживачів на телекомунікаційні послуги невпинно зростає, одночасно оголюючи проблеми цієї сфери та їх вплив на суспільство в цілому та особистість окремо. Все це залишається актуальним для українців.

У минулому 2020 р. кожен чітко побачив, що цифрове підключення є важливим у житті людей різних сфер доходу та різних країн світу.

Не так давно швидкісний доступ до Інтернету розглядався як «приємний у користуванні» для заможних та технічної еліти. COVID-19 перетворив його на необхідність для все більшої кількості людей - рятівний круг для соціально віддаленої роботи, школи, соціальних зв'язків і навіть консультацій з питань охорони здоров'я.

За даними ООН та Міжнародного союзу телекомунікацій протягом останніх п’ятнадцяти років частка населення світу, що мають доступ до Інтернету, сильно збільшилася – від 17 % до 50% орієнтовно. Але зменшення цифрового розриву не усунуло

існуючі бар'єри, адже включеними до Інтернету має бути вся інфраструктура держави, населеного пункту тощо; послуги мають бути доступні для усіх, незалежно від демографічних та інших ознак, соціальних умов, тощо. Крім того, надавачі та споживачі таких послуг, до яких входить ще й мобільний та фіксований зв'язок, телебачення, електронний банкінг тощо, мають володіти відповідними навичками роботи та спілкування, готовими до співпраці та взаємоповаги. Актуальним для світу, а України особливо, є наповнення цих каналів зв'язку відповідним контентом, що сприяє задоволенню потреб для життя та роботи, самовираження кожної людини, що гарантовано ст. 23, 34 Конституції України, та не порушує права і свободи інших, забезпечує соціально- економічний та політичний розвиток держави, захист її національних інтересів [2].

Звіт Світового економічного форуму про глобальні ризики на 2021 рік, який оголошений у Женеві, Швейцарія, у січні 2021 р., попереджає про нові небезпеки. Пандемія COVID – 19 збільшила відмінності не тільки у питаннях здоров'я, але й в економічних та цифрових технологіях. Мільярди людей можуть зупинитися на шляху до розвитку нового і справедливого суспільства, а це є особливо болючим для нашого сьогодення. Соціальна згуртованість може значно послабитися через нерівний доступ до технологічних та цифрових навичок. Останнє разом із розчарування молоді є частиною сучасної небезпеки (0-2 роки). У середньостроковій перспективі (3-5 рр.) респонденти прогнозують економічні ризики, зрив ІТ-інфраструктури.

Ст. 31 Конституції України та ст. 9, 32 ЗУ «Про телекомунікації» гарантують охорону таємниці будь – якої кореспонденції, захист інформації про споживача та безпеку телекомунікацій. У цьому питанні українці стикаються з величезною кількістю проблем, особливо на фоні зростання кіберзлочинів у всьому світі. Останні можуть вражати велику кількість підприємств та організацій у величезних ділянках географічних регіонів. Зокрема це відчули школи та університети світу під час широкомасштабного використання електронних платформ в умовах дистанційного навчання з весни 2020 р.

Законодавство гарантує кожній людині вільний та однаковий доступ до каналів зв'язку, захист її прав. Стан ринку телекомунікаційних послуг за 9 місяців 2020 року, оприлюднений на офіційному сайті Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформації,

свідчить, що структура доходів телекомунікаційних послуг за вказаний час зросла зокрема на 4527,2 млн грн для рухомого (мобільного) зв'язку та 992,8 млн грн для фіксованого доступу до мережі Інтернет, крім того збільшилася кількість ліній (точок) фіксованого доступу до мережі Інтернет на швидкості 10 Мбіт/с і більше паралельно із кількістю ліній з невизначеною оператором швидкості. При цьому розрив між сільською та міською місцевістю за кількістю ліній (точок) доступу до мережі Інтернет знизився на 11% [3]. Оприлюднені звіти про наданні послуги свідчать, що не всі суб'єкти господарювання сфери телекомунікацій долучаються до ознайомлення споживачів з рівнем своїх послуг, а певна частина (наприклад, 19 % інтернет провайдерів у 2019 р.) надає їх на нижчому рівні за граничний, встановлений законодавством. Але все це не забезпечує повноцінне залучення громадян до телекомунікаційних каналів в особистому чи суспільному просторі, реалізації своїх прав та свобод, не забезпечує потрібний доступ до різних послуг державних чи підприємницьких установ, економічного зросту держави. На сьогодні, Україну відносять до групи країн із середнім рівнем розвитку, причому ймовірність опинитися у числі слаборозвинених країн третьої групи зросла від 12% до 21 %, а ймовірність піднятися вище знизилася від 18 % до 8%.

За результатами дослідження глобальних мегатрендів міжнародною консалтинговою компанією KPMG «Майбутня держава 2030», що було проведене в 127 країнах світу, визначено дев'ять головних чинників впливу на розвиток держав у найближчі десятиліття. Серед них: розширення можливостей для особистості, високоефективна технологія, економічний взаємозв'язок, урбанізація та демографія, зміна балансу сил в економіці та інші. Глобальні мегатренди пов'язані між собою, їх вплив лише збільшуватиметься з часом, прискорюючи взаємозумовлені зміни в економічній, екологічній та соціальній сферах життєдіяльності як окремої особистості, так і всього суспільства. Визначені мегатренди адаптовані для країн з будь-якою територією, незалежно від регіону та рівня досягнутого добробуту. [4, с. 39-40]. Тому питання розвитку сфери телекомунікацій саме для України потребує великих фінансових та трудових ресурсів.

А Україна має не найкращі показники: за рівнем залучення інвестицій займаємо 121-ше місце серед 131 країн світу, верховенства права - 109, політичної стабільності - 123, розвиненістю бізнесу - 104. Саме на ці сфери варто звернути увагу при реформуванні національної економіки задля переходу на інноваційний шлях розвитку.

Зважаючи на вкрай низький рейтинг за індикатором «Верховенство права», для нас важливим є досвід провідних країн щодо захисту прав інтелектуальної власності. Адже в Угоді про Асоціацію між Україною та ЄС окремим розділом (глава 9) виділено співпрацю у сфері інтелектуальної власності. Україна була і залишається у переліку країн, які не забезпечують захисту прав інтелектуальної власності та щодо яких ведеться спостереження Управлінням торгового представника США — країна перебуває у групі країн Priority Watch List. Серед основних проблемних питань: широке використання неліцензійного програмного забезпечення українськими державними установами та невиконання ефективних засобів боротьби із широкомасштабним порушенням авторських прав в Інтернеті [5].

Величезна кількість каналів зв'язку сприяє підвищенню обізнаності та залученості, а також розширенню доступу до інформації, але існує небезпека виникнення певних труднощів, зокрема, вони посилюють співчуття та глобальну активність у сфері прав людини, але разом з тим виникає загроза появи ненависті, стереотипів та дезінформації. Особливо вразливими до онлайн-ризиків є діти та молодь.

Право на інформацію або право знати означає говорити про те, що широка громадськість повинна мати можливість брати участь у вільному потоці інформації і знати, що відбувається навкруги. Відповідно до Міжнародного пакту громадянського і політичного права, право на свободу висловлювання думок «передбачає свободу пошуку, отримання і поширення інформації та будь-яких ідей, незалежно від кордонів». Люди повинні мати вільний доступ до інформації, якою володіє влада. Крім того, в сучасному інформаційному суспільстві рівноправний доступ до освіти, професійної підготовки, науки, техніки та зайнятості може бути забезпечений, за умови виключення нерівності у доступі до інформації.

Але тут виникають нові ризики, які є постійними для українського суспільства та у напрямку усунення яких, на мою точку зору, не ведеться достатня робота. Мова йде про випадки, коли свобода вираження думки може вступити в конфлікт з іншими правами людини. До однієї групи прав людини належить право на конфіденційність, яке включає свободу від втручання в особисте і сімейне життя, житло і особисту кореспонденцію, а також право на захист честі та репутації.

Крім того, існує ризик виникнення конфлікту між свободою вираження думки і забороною дискримінації у

випадках, де реалізація прав свободи спрямована для розпал агресії і містить прояви мовної ворожнечі. За даними Комітету Міністрів Ради Європи, мова ворожнечі охоплює всі форми самовираження, які поширюються, підбурюють, сприяють або виправдовують расову ненависть, ксенофобію, антисемітизм або інші форми агресії, що призводять до нетерпимості і відсутності толерантності.

Свобода вираження думки не є абсолютним правом. Відповідно до статті 29 Загальної декларації права людини, реалізація прав і свобод може бути обмежена, якщо вони загрожують належному визнанню і повазі до прав і свобод інших осіб. Відповідно до статті 10 Європейської конвенції про захист прав людини (ЄКПЛ) реалізація права на свободу вираження думки з огляду на те, що вони відповідають основним обов'язкам і відповідальності громадян, може підлягати встановленими законом формальностям, умовам, обмеженням або санкціям, що є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету та неупередженості правосуддя.

Тому потрібно проводити регуляторну політику з метою дотримання норм законодавства, але при цьому можливий ризик обмеження прав та свобод людей авторитарними державами [6].

Питання розвитку телекомунікацій в Україні та світі, що впливають на соціальне середовище, задоволення людиною своїх потреб охоплено у статті частково. Проблеми потрібно вирішувати як короткострокові так і довгострокові, затребуваним є грамотне планування, регулювання, залучення фінансових та людських ресурсів. Президент Комітету з соціальних цінностей SK Group Лі Хен Хі наголошує, що стійкість економік та суспільств у всьому світі буде залежати від постійного зростання підключення до мережі, оскільки економіки, які оцифрувалися раніше, мали порівняно кращі результати у 2020 р.

Література:

1. Закон України «Про телекомунікації»(Відомості Верховної Ради (ВВР), 2004, N 12, ст.155) (Із змінами, внесеними згідно із Законом N 1876-IV (1876-15) від 24.06.2004).

2. https://www.weforum.org/focus

3. https://nkrzi.gov.ua/index.php?r=site/index&pg=1&language=uk

4. КРАЇНА 2030: Доктрина збалансованого розвитку, УКРАЇНА 2030: Доктрина збалансованого розвитку. Видання друге. — Львів: Кальварія, 2017. — 164 с.

5. Інтелектуальна власність – останній шанс на вихід із кризи, В.ХУСТОВ, вчений секретар ДУ «Інститут економіки та прогнозування НАН України», стаття газети ВР України «Голос України», 14.01.2021р.

6. Компас, Посібник з освіти в області прав людини за участі молоді https://www.coe.int/uk/web/compass/media#11

СОЦІАЛЬНО-ЕКОНОМІЧНІ ПИТАННЯ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙ

Руденко Дарина Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Комплексно розкрито питання розвитку телекомунікаційних мереж , що включає технологічні, організаційні та регуляторні аспекти створення та впровадження новітніх технологій.

Основні завдання розвитку телекомунікацій полягають в підвищенні ефективності використання телекомунікацій враховуючи, що ресурси можуть бути обмежені для їх розвитку. Створення нормативних, нормативно-правових, технічних документів, що регламентують всі питання, які пов'язані з функціонуванням телекомунікаційних мереж та суб'єктів сфери телекомунікацій.

Ефективність у сквері телекомунікацій залежить від уваги, яку приділяють технологічним та суспільним аспектам із реалізації.

Одна з найголовніших умов реалізації в сфері телекомунікацій є фінансова підтримку від держави.

Держава має забезпечити всіма необхідними технічними засобами. Наприклад, обладнання, кабельна продукція, програмні продукти. Вони сприятимуть високому досягненню технічного рівня телекомунікаційних мереж і будуть йти мінімальні витрати на їх реконструкцію та експлуатацію.

Забезпечення технічними засобами здійснюється шляхом тендерних заходів у вітчизняних та зарубіжних постачальників.

Для безперешкодного доступу суб'єктів телекомунікацій потрібно створити на державному рівні всі можливі умови.

Література:

1. «Власність Секретаріату Кабінету Міністрів України. Проект реалізовано Фондом Східна Європа та Державним агентством з питань електронного урядування України у межах програми міжнародної технічної допомоги "Електронне врядування задля підзвітності влади та участі громади" (EGAP) , за фінансової підтримки Швейцарської агенції розвитку та співробітництва.»; стаття, Київ, 2006; Електронний ресурс. Режим доступу: https://www.kmu.gov.ua/npas/39141641

ВПЛИВ ТЕЛЕКОМУНІКАЦІЙ НА ВЕДЕННЯ БІЗНЕСУ

Шостак Тетяна Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Однією із загальносвітових тенденцій є розвиток інформаційного суспільства.Технологіїмайбутньогострімкопроникають у повсякдення, стаючибільшінтегрованими і взаємопов'язаними. Динаміка цього процесу, його результати для громадян, суспільства та держави значною мірою залежать від обґрунтованості відповідної державної політки та управління, які повинні формуватись на основі достовірної, точної, своєчасної та повної інформації. На сьогодні розвиток інформаційного суспільства, поширення інформаційних технологій (ІТ) в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації. Практично всімафахівцями, економістами, політикамиусвідомлено, що розвиток ІТ створює засади сучасноїекономіки та добробутулюдини.

Телекомуніка́ції - це передавання та приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду дротовими, радіо, оптичними або іншими електромагнітними системами. Телекомунікація виникає при обміні інформацією між учасниками з використанням технологій. Передача відбувається або за допомогою електрики, що проходить через фізичному носії, як-от кабель, або за допомогою електромагнітного випромінювання. Зазвичай, шляхи передачі розділяють на канали зв'язку, що дозволяє користуватись перевагами мультиплексування. Термін часто використовується в множині, тобто телекомунікації, тому що для передачі використовуються багато різних технологій.[1]

Найбільш повне та суттєве тлумачення поняття інформатизації надано у ЗаконіУкраїни «Про національну программу інформатизації». В ньому наголошується, що «інформація є сукупністю взаємопов’язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, які направлені на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку та використання інформаційних систем, мереж, ресурсів та інформаційнихтехнологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки» [2].

«У сучасному мінливому світі, де завдяки діджиталізації зміни відбуваються буквально щохвилини, надзвичайно важливо тримати руку на пульсі. Бізнесу особливо необхідно стежити за світовими трендами та інтегруватиїх у свої процеси, аби не опинитися на узбіччі. Дослідження «Делойт» покликане

допомагати бізнесу у прийнятті стратегічних управлінських рішень. Зокрема, зрозуміти, на як іновації варто звертати увагу й вивчати особливості їхнього функціонування на перспективу, а які технології треба імплементувати вже зараз, аби трансформувати свої підходи до ведення бізнесу і таким чином підвищувати його ефективність», – коментує Володимир Юмашев, партнер, лідер індустріальної групи технологій, медіа та телекомунікацій «Делойт» в Україні.

Концепція розвитку телекомунікацій в Україні до 2010 року відповідно до Закону України "Про телекомунікації" визначає основні засади і напрями подальшого розвитку телекомунікаційних мереж загального користування (далі — телекомунікаційнімережі) в ринкових умовах і спрямована на досягнення стратегічних інтересів та конкурентоспроможності України на міжнародному ринку.

Стратегія розвитку телекомунікаційних мереж повинна базуватися на використанні новітніх технологій, які відповідають міжнародним стандартам, враховувати необхідність технологічної взаємодії всіх мереж при наданнітелекомунікаційнихпослуг, забезпечити підвищення ефективності їх функціонування. Телекомунікації відіграють значну роль в соціальній та економічній діяльності суспільства, забезпечуючи оперативне або інтерактивне (діалогове) передавання інформації.

Розвиток телекомунікацій повинен здійснюватися випереджувальними темпами порівняноіз загальними темпами розвитку економіки і буде визначальним на найближчу і більшвіддалену перспективу. Повільні темпи розвитку телекомунікацій спричиняють зниження конкурентоспроможності економіки України. Телекомунікації відіграють значну роль у прискоренні розвитку економіки та соціальної сфери.[4]

З метою прискорення розвитку телекомунікаційних мереж слід створити сприятливі умови для добросовісної конкуренції на ринку телекомунікаційних послуг, підвищити його інвестиційну привабливість, забезпечити прозорість взаємовідносин суб'єктів ринку телекомунікаційних послуг, консолідувати їх зусилля на розв'язання проблем розвитку телекомунікацій.Прискорений розвиток телекомунікацій є одним із основних чинників, що впливатиме на розбудову національної економіки та масове впровадження інформаційних технологій, побудову в Україні інформаційного суспільства, на процесс інтеграції України в ЄС та у світову економіку, а також збільшення надходжень до державного бюджету.

Література:
1 Телекомунікації — Вікіпедія (wikipedia.org)
2. ZakonUkrainy «Pro natsionalnuinformatyzatsiiu». [Elektron. resurs]. Rezhymdostupu:http://zakonl.rada.gov.ua/laws/show/1280-15
3. https://www2.deloitte.com/ua/uk/pages/about-deloitte/articles/2020-tmt-predictions.html
4. https://www.kmu.gov.ua/npas/39141641

ПРОБЛЕМИ РОЗВИТКУ ГАЛУЗІ ТЕЛЕКОМУНІКАЦІЙ У СУЧАСНИХ УМОВАХ

Ярцева Дар'я Дмитрівна
Дежавний Університет Телекомунікацій
Навчально-науковий інститут Менеджменту та підприємництва
м. Київ

Сьогодні стає загальновизнаним той факт, що засоби телекомунікацій знаходяться на етапі перетворення, який охопив системи і мережі електрозв'язку та інформаційні послуги, які вони надають.

Розвиток галузі телекомунікацій визначається лібералізацією та глобалізацією ринку телекомунікації. Лібералізація зумовлена переходом від монопольної структури надання послуг до конкурентного середовища і, як наслідок, зростанням кількості операторів недержавної або змішаної форм власності та кількістю мереж, заснованих на сучасних технологіях.

Основними пріоритетами розвитку галузі зв'язку в Україні є:

• Забезпечення розвитку телефонних мереж шляхом завершення створення цифрових мереж, прискорення переобладнання існуючих мереж на базі новітніх технологій і цифрового обладнання.

• Впровадження нових видів послуг та нових технологій оброблення, перевезення і доставки усіх видів поштових відправлень на основі комплексної механізації та автоматизації виробничих процесів у поштовому зв'язку, використанні комп'ютерних методів оброблення повідомлень.

• Дослідження, розробка та впровадження нових принципів організації зв'язку, організація розроблення та виробництва в Україні основних видів технічних засобів зв'язку на рівні європейських і світових стандартів якості.

Виконання таких завдань ставить нові вимоги по кадровому забезпеченню та науково-технічному розвитку галузі. Перед закладами освіти постає задача підготовки, перепідготовки та підвищення кваліфікації фахівців для галузі телекомунікацій, де освітянський рівень працівників галузі,

сформований ще 10-20 років тому, не відповідає зростанню технологічної бази та новітніх засобів телекомунікацій.

Особливо гостро проблема підготовки фахівців стоїть для підгалузі поштового зв'язку. Підготовкою спеціалістів для поштового зв'язку не займається жодна установа вищої освіти в Україні. Серед керівних та інженерно-технічних робітників підгалузі поштового зв'язку дуже низька доля фахівців з вищою освітою з поштового зв'язку (менше 3 %).

Незважаючи на те, що галузь телекомунікацій та інформаційних технологій надзвичайно капітало- та науковомістка і в неївже залучено значні суми, цих інвестицій замало, враховуючи потенціал країни. Можна говорити про два моменти, які об'єктивно пояснюють недостатній рівень інвестування в телекомунікації в Україні: незадовільне законодавче забезпечення діяльності інвесторів та слабка державна підтримка цьому процесу.

Отже, потреба України в інвестиціях та становленні сучасного зв'язку може бути забезпечена шляхом об'єднання зусиль усіх структур галузі телекомунікацій, включаючи уряд. Основою для інвестування вітчизняного та іноземного капіталу і кредитів мають стати продумане планування та тісна співпраця учасників галузі. Але відкриття ринку послуг іноземним компаніям у розвинених країнах допускається тільки за мірою достатнього його насичення послугами, що надаються національними операторами. Такий підхід дозволяє підвищити конкурентоспроможність національних операторів, підготувати їх до умов відкритого ринку та уникнути зайняття домінуючих позицій іноземними операторами.

Нині ринок інформаційних і телекомунікаційних технологій - один з найбільш прибуткових секторів економіки України, що динамічно розвивається. Проте досягнутий рівень телефонізації досить низький у порівнянні з показниками розвинених країн.

Література:

1. Латік В. Основніпоказникирівняжиттянаселення // Праця і зарплата, 2005. - №10. - С. 2.

2. Довгаль О.Г. Соціальніпослуги , як елементринковоїінфраструктури //Формування ринковихвідносин в Україні, 2003. - № 7-8.

ЗАСТОСУВАННЯ МЕТОДІВ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ОПТИМІЗАЦІЇ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Ющенко Анастасія Юріївна
Державний університет телекомунікацій
Навчально-науковий інститут телекомунікацій

Власик Ганна Миколаївна
Державний університет телекомунікацій
Навчально-науковий інститут гуманітарних
та природничих дисциплін
м. Київ

Економічна безпека є необхідною умовою існування будь-якого підприємства, вона забезпечує захищеність його життєво важливих інтересів від внутрішніх і зовнішніх загроз та є підґрунтям стійкого функціонування.

Поняття «економічна безпека» пройшло чимало переосмислень у зв'язку зі зміною умов зовнішнього середовища і з урахуванням факторів, які зумовлюють процеси управління. Економічну безпеку підприємства можна розглядати як одну з складових загального поняття «безпека». ***Економічна безпека підприємства*** – це захист діяльності підприємства від негативних впливів зовнішнього середовища, а також здатність швидко усувати різноманітні загрози чи пристосовуватися до існуючих умов, які не позначаються негативно на його діяльності. Крім того, економічна безпека підприємства – це найефективніше використання ресурсів, які забезпечують стабільне функціонування підприємства.

У ринкових умовах господарювання економіко-математичні методи стають важливим інструментом отримання більш глибоких і повних знань про кількісні та якісні сторони економічного механізму тих чи інших процесів та явищ. Стратегічні рішення необхідно приймати не інтуїтивно, а на підставі всебічного статистичного аналізу та математичних розрахунків. Не випадково, що саме в наш час, відзначається посилений інтерес до використання математичних методів у макро- та мікроекономічних дослідженнях. Замість того, щоб «пробувати і помилятися» на реальних об’єктах, аналітики віддають перевагу робити це за допомогою економіко-математичних моделей.

Моделювання – це процес побудови моделі, за допомогою якого вивчається функціонування об’єктів різної природи. Він складається з трьох основних елементів: суб’єкта, об’єкта дослідження та моделі, з допомогою якої суб’єкт пізнає об’єкт. Моделювання служить передумовою та інструментом аналізу економіки і процесів, які функціонують у ній, а також як засіб обґрунтування прийняття рішень, прогнозування, бізнес-планування та керування економічними об’єктами. Модель економічного об’єкта переважно підтримується реальними статистичними та емпіричними даними, а результати розрахунків, виконані в межах побудованої моделі, дають

можливість будувати прогнози на майбутнє та давати об’єктивні оцінки корисності об’єктів дослідження.

Найбільш важливими моделями, що використовуються при дослідженні розвитку та функціонування економічних процесів є математичні. Будь-яка модель задачі для дослідження окремого класу включає в себе змінні, систему обмежень і мету. Мета – це цільова функція, яка задається на множині допустимих розв’язків *D*. Сама множина *D* виражає міру досягнення мети: якщо *D* – пуста множина, то розв’язків не існує; якщо *D* – одна точка, то ця точка буде єдиним допустимим розв’язком задачі, який не представляє собою для нас інтересу; якщо *D* містить більше одного розв’язку, то *задача оптимізації полягає у знаходженні оптимального розв’язку* на множині допустимих. При цьому, якщо *D* скінченна, то оптимальний розв’язок може бути знайденим у результаті простого перебору всіх точок *D*, для яких визначаються значення цільової функції. Тому, при побудові моделей економічних систем, слід відображати тільки найважливіші та найхарактерніші властивості процесів або явищ, що вивчаються. Внаслідок цього всі моделі є спрощеним відображенням реальної системи, але якщо цей процес виконано коректно, то отримане наближене відображення реальної ситуації дає можливість мати достатньо точні характеристики об’єкта дослідження.

	Натуральний еквівалент	Грошовий еквівалент	Коментарі
Поріг рентабельності	572 шт.	57 200 грн	При реалізації товару менше, ніж 572 одиниці товару або при виручці менше 57 200 грн, підприємство буде мати збиток
Запас фінансової міцності	1 422 шт.	142 800 грн	Якщо заробляти на 123 800 грн менше або продавати на 1 422 одиниць товару менше, підприємство матиме збиток
Сила операційного	1,4		Наприклад, при збільшити виручку на 10%, то прибуток зросте

важеля		на 14%, а от при зменшенні виручки на 10% - прибуток зменшиться на 14%

Розглянемо ***задачу*** при наступних вихідних даних:

Ціна реалізації одиниці продукції	100 грн
Річний обсяг реалізації продукції	2 000 шт.
Змінні витрати на одиницю продукції	65 грн
Прямі постійні витрати	15 000 грн
Непрямі постійні витрати	5 000 грн

Розрахуємо поріг рентабельності, запас фінансової міцності і силу операційного важеля:

Ці основні критерії оцінки економічної безпеки підприємства дають відповідь на яку мінімальну кількість товару можна реалізовувати, щоб не мати збитку. Або, наприклад, як зміниться прибуток підприємства від збільшення чи зменшення кількості реалізованої продукції.

Отже, математичне моделювання деякою мірою забезпечує оптимізацію рівня економічної безпеки підприємства. Для зменшення ризиків негативних факторів слід надати перевагу саме науковій дисципліні, яка займається розробкою та практичним використанням математичного апарату.

Література:

1. Гнилицька Л. Основи економічної безпеки підприємства // Бухгалтерський облік і аудит: Економічна безпека підприємства. - 2013. - №7. - С. 41 - 48.

2. Економічна безпека підприємства: навчальний посібник / Небава М.І., Міронова Ю.В. – Вінниця: ВНТУ, 2017. – 73с.

3. Економіко-математичне моделювання: Навчальний посібник / за ред. О.Т. Іващука. – Тернопіль: ТНЕУ «Економічна думка», 2008. – 704 с.

Наукове видання

«СВІТ ТЕЛЕКОМУНІКАЦІЇ ТА ІНФОРМАТИЗАЦІЇ»

Збірник матеріалів
XI Міжнародної науково-технічної конференції студентства та молоді

Київ, 19 лютого 2021 року

Редагування: Іпатов Г.Г., Пришко С.А.
Відповідальні за випуск: Іпатов Г.Г., Ожигін Н.В., Левандовська В.А., Парфенюк Т. М., Ціпов'яз К. Д.

Подано до друку 25.02.2021
Формат 60х84. Папір друкарський. Гарнітура «Time New Roman».

Державний університет телекомунікацій
вул. Солом'янська, 7, м. Київ, 03110, Україна

Для нотаток

Для нотаток

LEADERS OF STUDENT'S COUNCIL

STATE UNIVERCITY OF TELECOMMUNICATIONS

SINCE 2009

Контакти

dut.edu.ua

lsd.dut.edu.ua