ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «ДОСЛІДЖЕННЯ МЕТОДИКИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІОТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ»

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Данило КОНДРАТЕНКО
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Данило КОНДРАТЕНКО
здобувач вищої освіти
група ІСДМ-63

Керівник: Ольга ПОЛОНЕВИЧ
науковий ступінь, вчене звання к.т.н., доцент

Рецензент:
науковий ступінь, вчене звання

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

Ступінь вищої освіти Магістр

Спеціальність Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС

_____ Каміла СТОРЧАК
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кондратенко Данило Володимирович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методики захисту інформації в мережі IoT від несанкціонованого доступу.

керівник кваліфікаційної роботи Ольга ПОЛОНЕВИЧ к. т. н., доцент,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» 10.2023р. №145

2. Строк подання кваліфікаційної роботи «29» грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, технічна документація систем захисту інформації, вимоги до комплексних систем захисту інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз специфік архітектурних рівнів для захисту інформації в мережі інтернету речей
Апаратне забезпечення безпечної системи інтернету речей

Програмне забезпечення безпечної системи інтернету речей

5. Перелік графічного матеріалу: *презентація*
    1. Теоретична частина та аналіз специфікацій
    2. Апаратні складові систем
    3. Програмного забезпечення систем

6. Дата видачі завдання«19» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	19.10-05.11.23	
2	Вивчення теоретичних основ інтернет медичних речей	05.11-12.11.23	
3	Дослідження технічних аспектів захисту інформації, та стандартів	13.11-18.11.23	
4	Аналіз проблем впровадження систем захисту інформації, та систем комплексного захисту інформації	19.11-23.11.23	
5	Огляд практичного впровадження та прикладів застосування СЗІ та КСЗІ	24.11-03.12.23	
6	Аналіз оптимальних технологій для забезпечення безпечної системи IoT	04.12-10.12.23	
7	Оформлення роботи: вступ, висновки, реферат	11.12-20.12.23	
8	Розробка демонстраційних матеріалів	21.12-29.12.23	

Здобувач вищої освіти _____ Данило КОНДРАТЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Ольга ПОЛОНЕВИЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 68 стор.,39 рис., 74 джерел.

Мета роботи – детальне дослідження та розробка методів захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу.

Об'єкт дослідження – є система захисту інформації в мережі IoT від несанкціонованого доступу.

Предмет дослідження – методики захисту інформації в мережі IoT та архітектура мережі для ефективного виявлення та обмеження несанкціонованого доступу.

Короткий зміст роботи: робота зосереджена на розробці та вивченні ефективних методів захисту інформації в мережі Інтернету речей від несанкціонованого доступу. Включає аналіз архітектури IoT, вивчення різних методів захисту інформації, та розгляд актуальних викликів у сфері інформаційної безпеки.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, ЗАХИСТ ІНФОРМАЦІЇ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ІОТ-СИСТЕМИ.

ABSTRACT

The text part of the qualifying work for obtaining a master's degree: 68 pages, 39 figures, 74 sources.

Purpose – to comprehensive research and development of methods for protecting information in the Internet of Things (IoT) network from unauthorized access.

The object of research is the information security system in the IoT network against unauthorized access.

The subject of this research is the methods of information protection in the IoT network and the network architecture for effective detection and limitation of unauthorized access.

Summary of work: Analysis of scientific papers, books, conferences, and other sources to understand the current state of IoT in healthcare and examines specific cases of successful IoT solution implementation.

KEYWORDS: INTERNET OF THINGS, INFORMATION SECURITY, UNAUTHORIZED ACCESS, IOT SYSTEMS.

ЗМІСТ

ВСТУП

За останні роки спостерігається значний приріст кількості підключених до мережі IoT-пристроїв, включаючи розумні домашні пристрої, медичні пристрої, автомобільні системи та промислові IoT-рішення. Зі зростанням кількості пристроїв збільшується потенційна поверхня для атак.

IoT-пристрої обробляють і передають різноманітну інформацію, включаючи особисті дані, медичні записи та виробничі дані. Захист цих даних стає критично важливим для уникнення порушень конфіденційності та можливого зловживання.

Актуальність теми полягає у забезпечення безпеки в мережі Інтернету речей (IoT) від несанкціонованого доступу визначається не лише розширенням самої IoT, але й різноманітністю і значущістю даних, які обробляються цими системами. IoT використовується в різних галузях, включаючи медицину, транспорт, промисловість та побут, і важливо захистити конфіденційні дані, інтегрітету систем і забезпечити доступність сервісів.

Метою магістерської роботи є проведення докладного дослідження та вивчення методик захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу. Ключовою метою є розробка та вдосконалення стратегій, технологій та методів захисту, спрямованих на забезпечення конфіденційності, цілісності та доступності даних в IoT-системах.

Об'єктом дослідження є система захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу.

Предметом дослідження є методики захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу. Вивчення та вдосконалення архітектури мережі IoT для ефективного виявлення та обмеження несанкціонованого доступу.

Джерелами дослідження є методики захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу використовуються різноманітні джерела. Огляд матеріалів конференцій, таких як Black Hat, DEFCON, IEEE International Conference on Internet of Things (IoT), для виявлення новітніх розробок та тенденцій у галузі. Аналіз технічної документації виробників IoT-пристроїв та платформ для вивчення рекомендацій з їхньої безпеки.

Практична цінність дослідження методик захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу має широкий спектр проявів та можливість впливати на різні аспекти сучасного інформаційного середовища. Покращення захисту може стимулювати розвиток та використання IoT-рішень в різних галузях, дозволяючи більш широкий та безпечний застосунок цих технологій. Забезпечення безпеки в IoT допомагає захистити фізичну та цифрову інфраструктуру, зменшуючи ризик негативного впливу на роботу пристроїв та систем.

Апробація дослідження здійснювалась у формі участі в загальногалузевому науково-виробничому журналі «Зв'язок» та ауково-практичній конференції «Telecommunication: problems and innovation»*Структура роботи.* Загальний обсяг роботи 68 сторінок друкованого тексту. Дана робота складається зі вступу, трьох розділів, висновків, списку використаної літератури, що включає 74 одиниць. Текст містить 39 рисунків та 1 таблиці. Робота буде корисною для результатів дослідження забезпечення нових або вдосконалених методик захисту в Інтернеті речей, що може враховувати сучасні загрози та виклики, робить важливий внесок у розвиток цієї сфери.

РОЗДІЛ 1. АНАЛІЗ СПЕЦИФІК АРХІТЕКТУРНИХ РІВНІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

1.1. Визначення актуальності проблеми захисту IoT

Архітектура Інтернету речей (IoT) визначається як структура та організація системи, яка включає в себе підключені до мережі фізичні об'єкти та їх взаємодію. Архітектура IoT розробляється з метою забезпечення ефективності, безпеки, масштабованості та іншими аспектами, щоб забезпечити оптимальну роботу великої кількості підключених пристроїв.

Інтернет речей (IoT) – це система взаємопов'язаних обчислювальних пристроїв, механічних і цифрових машин, предметів, тварин або людей, які мають унікальні ідентифікатори (UID) та можливість автоматично оновлювати дані через мережу без прямого втручання людини. Така система дозволяє об'єднувати фізичний світ з цифровим, надаючи можливість збору, обробки та обміну інформацією для полегшення різних аспектів повсякденного життя та виробничих процесів.

Основні елементи архітектури IoT включають:

Фізичні пристрої, що забезпечують здатність вимірювати, збирати дані (сенсори) та впливати на навколишнє середовище (актуатори).

Системи для збору, передачі та обробки даних від сенсорів, що може включати в себе різні комунікаційні протоколи та мережеві технології.

Інфраструктура для обробки та аналізу даних, яка може бути розташована як в центрі хмари, так і на краю мережі (edge computing), щоб забезпечити більш швидку відповідь та зменшити обсяг даних що передаються.

Технології для підключення пристроїв в IoT мережу, включаючи бездротові (Wi-Fi, Bluetooth, Zigbee) та дротові (Ethernet) засоби зв'язку.

Системи для управління та керування IoT-пристроями, включаючи реєстрацію, аутентифікацію, моніторинг та управління доступом.

Використання аналітики та штучного інтелекту для отримання значущої інформації з великих обсягів даних, а також для прийняття автоматизованих рішень.

Заходи безпеки для захисту від несанкціонованого доступу, атак та забезпечення конфіденційності інформації.

Забезпечення можливостей взаємодії з IoT за допомогою додатків та інтерфейсів.

Інтернет речей стає невід'ємною частиною сучасного технологічного ландшафту. З кожним роком збільшується кількість підключених пристроїв та систем, що підвищує ризик кіберзагроз.

1.2. Визначення та опис архітектури IoT

Варто зазначити, що єдиної архітектури IoT не існує. Вона залежить від складності та кількості шарів архітектури конкретного бізнес-завдання.

Наприклад, модель додатків, анонсована компаніями Cisco в 2014 році IBM і Intel на IoT World Forum 2014 включає до семи рівнів. Відповідно до офіційного прес-релізу головних форумів Cisco, ціль цієї архітектури: «Допомога навчити IT-директорів, IT-відділи та розробників», розгортання проєкту IoT та прискорення впровадження IoT» [2].

Рис. 1.1. Ієрархічна модель Інтернету Речей

Але незалежно від варіанту використання та кількості рівнів, основні компоненти будь-якої структури Інтернету речей завжди однакові (рис. 1.1):

– розумні речі;
– мережі та шлюзи, які дозволяють пристроям з обмеженим енергоспоживанням, що часто характерне для Інтернету речей (IoT), з'єднуватися з розгалуженою мережею Інтернету;
– платформи проміжного програмного забезпечення для Інтернету речей, які надають резервуари для зберігання даних, розвинуті обчислювальні ресурси та аналітичні можливості;
– застосунки, що дозволяють кінцевим користувачам отримувати переваги від Інтернету речей та управляти фізичним оточенням (рис.1.2).

Рис. 1.2. Основна структура архітектури Інтернету Речей

Ці компоненти становлять основу будь-якої системи Інтернету Речей, на основі якої може бути розроблена ефективна багатошарова структура. Зазвичай це включає такі рівні:

– рівень засвоєння, де вміщуються розумні пристрої;
– рівень зв'язку або транспортний рівень, що передає дані між фізичним рівнем та хмарою через мережі та шлюзи;
– рівень обробки, який використовує платформи Інтернету Речей для накопичення та керування всіма потоками даних;

– прикладний рівень, що забезпечує функціонал, такий як аналітика, звітність та управління пристроями для кінцевих користувачів.

Поза основними компонентами, можуть бути додаткові шари:

– рівень обчислювального краю або туману, який виконує попередню обробку даних близько до місця збору інформації від речей IoT. Зазвичай, інтенсивні обчислення здійснюються на шлюзах;
– діловий рівень, де бізнес приймає рішення на основі зібраних даних;
– рівень захисту, що охоплює всі інші рівні.

Часто розглядані як необов'язкові, ці додаткові компоненти, тим не менше, надають проєкту Інтернету Речей відмінну придатність для сучасних бізнес-потреб [2].

Рівень сприйняття: конвертація аналогових сигналів у цифрові дані та навпаки.

На початковому етапі будь-якої системи Інтернету Речей охоплює широкий спектр "речей" або кінцевих пристроїв, які діють як місток між реальним та цифровим світами. Вони розрізняються за формою та розмірами – від крихітних силіконових чіпів до великих транспортних засобів. За своїми функціями речі Інтернету Речей можна поділити на такі великі групи.

Наприклад, датчики, такі як зонди, сенсори та лічильники, збирають фізичні параметри, такі як температура чи вологість, конвертують їх у електричні сигнали та передають у систему Інтернету Речей. Сенсори Інтернету Речей, зазвичай, мають невеликі розміри та витрачають мало енергії. Пускачі перетворюють електричні сигнали із системи Інтернету Речей у фізичні дії. Вони використовуються в контролерах двигунів, лазерах, роботизованих пристроях. Машини та пристрої, що підключені до датчиків та виконавчих механізмів або є їх невід'ємними частинами.

Важливо зауважити, що архітектура не обмежує сферу застосування її компонентів або їх розташування. Крайовий шар може включати лише кілька "речей", фізично розміщених в одній кімнаті, або безліч датчиків та пристроїв, розподілених по всьому світу.

Рівень підключення: забезпечення передачі даних

Другий рівень відповідає за усі взаємодії між пристроями, мережами та хмаровими сервісами, що формують інфраструктуру Інтернету Речей. Забезпечення комунікації між фізичним рівнем та хмарою реалізується двома способами:

– прямо, використовуючи стек TCP або UDP/IP.
– через шлюзи – апаратні або програмні модулі, які виконують трансляцію між різними протоколами, а також забезпечують шифрування та дешифрування даних Інтернету Речей (рис.1.3).

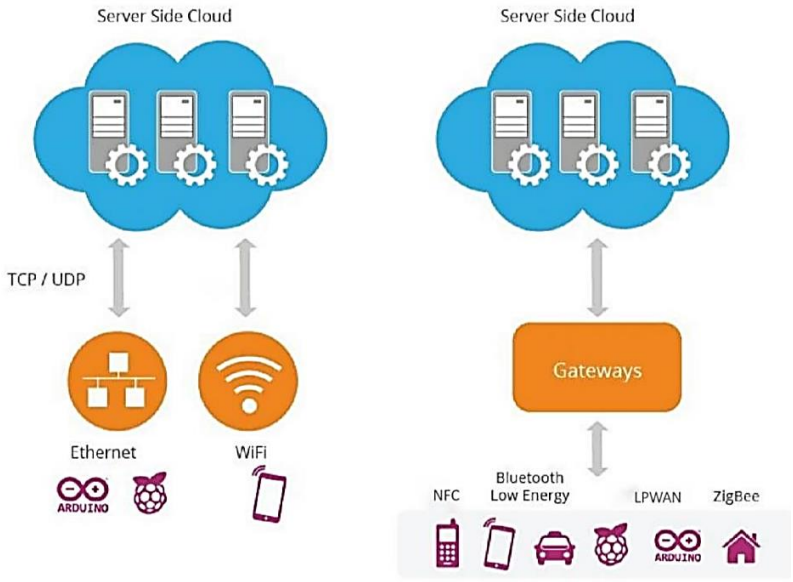


Рис.1.3. Комунікація від фізичного рівня до хмарових послуг.

Взаємодія між пристроями та хмарними службами або шлюзами включає в себе використання різноманітних мережевих технологій:

– *Ethernet* використовується для підключення стаціонарних або постійно розташованих пристроїв Інтернету Речей, таких як охоронні та відеокамери, а також промислове обладнання та ігрові консолі.
– *WiFi* найпопулярніша технологія бездротових мереж, ідеально підходить для рішень, які вимагають обробки великих обсягів даних IoT та працюють на обмеженій території, наприклад, у розумних домашніх пристроях.
– *NFC (Near Field Communication)* забезпечує простий та безпечний обмін даними між двома пристроями на невеликій відстані (10 см або менше).

- *Bluetooth* використовується для зв'язку на короткій відстані, особливо популярний серед переносних пристроїв. Стандарт Bluetooth Low-Energy (BLE) був розроблений для малопотужних пристроїв IoT, передаючи невеликі порції даних і працюючи ефективно для малих файлів.
- *LPWAN* (малопотужна широкосмугова мережа) спеціально розроблена для пристроїв IoT, забезпечує бездротове підключення на великій площі при низькому споживанні енергії, що дозволяє довготривалу автономну роботу.
- *ZigBee* бездротова мережа для передачі невеликих пакетів даних на короткі відстані, особливо ефективна для домашньої автоматизації та малопотужних пристроїв в промисловості, науці та медицині.
- *Стільникові мережі* пропонують надійну передачу даних та майже глобальне покриття для пристроїв IoT. Стандарти, такі як LTE-M та NB-IoT, відповідають різним потребам, дозволяючи обмін великими обсягами даних або передачу невеликих пакетів через низькочастотні канали[2].

Як тільки складові рішення Інтернету речей підключені до мережі, їм все ще необхідні протоколи обміну повідомленнями для передачі даних між пристроями та хмаровим сервісом. Серед найпопулярніших протоколів, використовуваних у сферах IoT, можна виділити *DDS, AMQP, CoAP, MQTT.*

Обчислювальний рівень хмари: зменшення затримки системи

Даний рівень є важливим для того, щоб системи Інтернету речей (IoT) відповідали вимогам щодо швидкості, безпеки та масштабування, які визначені новим стандартом бездротового зв'язку - мережею 5-го покоління або 5G. Такий стандарт обіцяє покращену швидкість, зменшену затримку та здатність обробляти значно більше підключених пристроїв, ніж поточний стандарт 4G.

Суть обчислень на рівні краю (Edge Computing) полягає в тому, щоб обробляти та зберігати інформацію як найближче до її джерела та як найраніше. Даний підхід дозволяє аналізувати та трансформувати великі об'єми даних в реальному часі на межі мережі. Таким чином, досягається зменшення затримки системи, що призводить до реакцій у режимі реального часу та підвищення продуктивності.

Обчислення краю відбуваються на шлюзах, локальних серверах або інших крайових вузлах, розподілених у мережі. На цьому рівні дані можуть бути:

- оцінені для визначення необхідності подальшої обробки на вищих рівнях;
- відформатовані для подальшої обробки;
- розшифровані;
- відфільтровані;
- перенаправлені на додатковий пункт призначення.

Підсумовуючи, перші три шари бачать дані в русі, оскільки вони постійно рухаються та змінюються. Лише після досягнення наступного рівня дані остаточно перебувають у стані спокою та доступні для використання споживчими програмами.

Рівень обробки: переформатування необроблених даних у корисні

Шар обробки виконує функції збирання, збереження та обробки даних, які надходять із попереднього шару. Зазвичай ці завдання реалізовані на платформах Інтернету речей (IoT) і включають два основні етапи.

Етап накопичення даних:

- Дані в режимі реального часу фіксуються за допомогою API і перебувають у стані спокою, щоб відповідати вимогам програм, що працюють не в режимі реального часу. Компонент накопичення даних діє як транзитний вузол між генерацією даних на основі подій та споживанням даних на основі запитів.
- Покладаючись на етап накопичення даних, визначається відповідність даних бізнес-вимогам та місце для їх зберігання. Дані зберігаються в різноманітних рішеннях для зберігання, від сховищ даних, здатних утримувати неструктуровані дані, такі як зображення та відеопотоки, до сховищ подій та телеметричних баз даних. Основна мета – ефективно відфільтрувати та зберегти різноманітні дані.

Етап абстракції даних

На цьому етапі підготовка даних завершена для використання споживчими програмами з метою отримання статистичних даних. Процес включає наступні кроки:

- Поєднання даних з різних джерел, як Інтернет речей (IoT), так і не IoT, включаючи системи управління відносинами з клієнтами (CRM), системи управління ресурсами підприємства (ERM) та інші.
- Узгодження різних форматів даних.
- Агрегація даних в одному місці або забезпечення доступу до них незалежно від їхнього розташування за допомогою віртуалізації даних.
- Переформатування даних, зібраних на рівні програм, для відправлення на фізичний рівень, щоб пристрої могли їх зрозуміти.

Разом етапи накопичення та абстрагування даних спрощують взаємодію між смарт-пристроями, а також дозволяють розробникам програм зосередитися на вирішенні конкретних бізнес-завдань, замість заглиблення в технічні характеристики пристроїв різних виробників.

Прикладний рівень: задоволення бізнес-вимог

На цьому рівні інформація аналізується програмним забезпеченням для відповіді на ключові ділові питання. Існують різноманітні програми Інтернету речей, що відрізняються за складністю та функцією, використовуючи різні технологічні стеки та операційні системи. До них відносяться:

- Програмне забезпечення для контролю та управління пристроями.
- Мобільні застосунки для простої взаємодії.
- Служби ділової розвідки.
- Аналітичні рішення, які використовують машинне навчання.

На сьогоднішній день можна розробляти додатки прямо на платформах IoT, що надають інфраструктуру розробки програмного забезпечення з готовими інструментами для видобутку даних, вдосконаленою аналітикою та візуалізацією даних. Інакше програми IoT використовують API для інтеграції з інтерфейсами програмного забезпечення (рис.1.4).

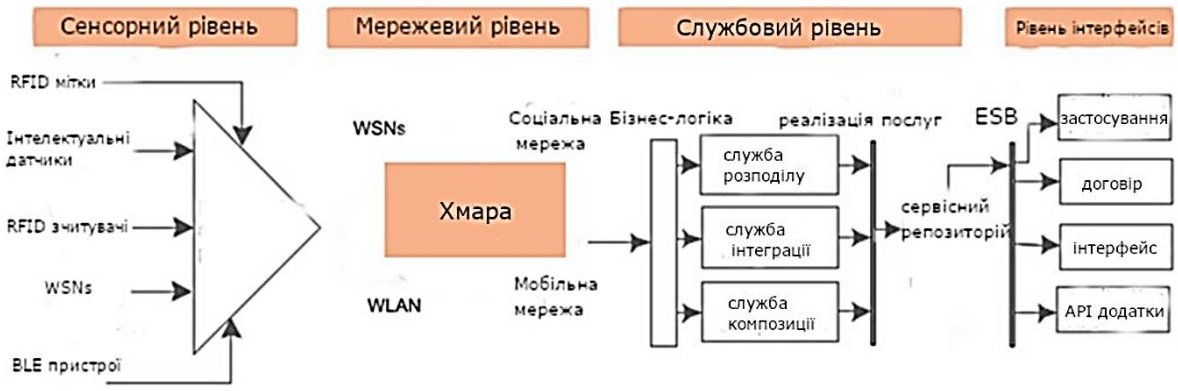


Рис. 1.4. Сервіс-орієнтована архітектура для IoT

Бізнес-рівень: впровадження рішень, керованих даними

Інформація, яка формується на попередніх рівнях, стає цінною лише в тому випадку, якщо вона призводить до вирішення проблем та досягнення бізнес-цілей. Нові дані повинні викликати співпрацю між зацікавленими сторонами, які, в свою чергу, впроваджують нові процеси для підвищення продуктивності.

На рівні прийняття рішень зазвичай бере участь не одна людина, яка працює з кількома програмними рішеннями. З цієї причини бізнес-рівень визначається як окремий етап, що виходить за межі окремого додатка.

Рівень безпеки: запобігання порушенням даних

Безпека на рівні Інтернету речей (IoT) включає в себе широкий спектр заходів і заслуговує окремого розгляду. Однак основні особливості безпечної архітектури на різних рівнях можуть бути визначені.

Безпека пристрою. Виробники сучасних пристроїв IoT інтегрують функції захисту в апаратне та програмне забезпечення, включаючи вбудовані мікросхеми TPM (Trusted Platform Module) для автентифікації та безпеки пристроїв кінцевих точок, безпечний процес завантаження, регулярні оновлення виправлень безпеки та фізичний захист.

Безпека з'єднання. Дані, які передаються через пристрої, мережі або програми, повинні бути зашифровані. Протоколи обміну повідомленнями, такі як MQTT, AMQP та DDS, можуть використовувати TLS (Transport Layer Security) для захисту даних.

Хмарна безпека. Дані, що знаходяться у хмарі в стані спокою, також повинні бути зашифровані. Хмарна безпека також включає механізми автентифікації, авторизації та управління ідентифікацією пристрою для обмеження доступу до програм IoT.

Рішення IoT від провідних постачальників мають вбудовані заходи захисту, але завжди важливо забезпечувати безпеку на всіх рівнях – від найменших пристроїв до складних аналітичних систем.

1.3. Математичні визначення безпеки систем.

Математична модель безпеки – це формальне визначення політики безпеки (рис.1.5). Згідно вимог нормативних документів у галузі захисту інформації в інформаційних системах, системи захисту інформації будуються на основі математичних моделей, які дозволяють теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки. Розвиток формальної теорії захисту інформації, хоч і недавній, вже призвів до створення численних математичних моделей, що описують різні аспекти безпеки та надають теоретичну базу для побудови сучасних систем захисту інформації [3].

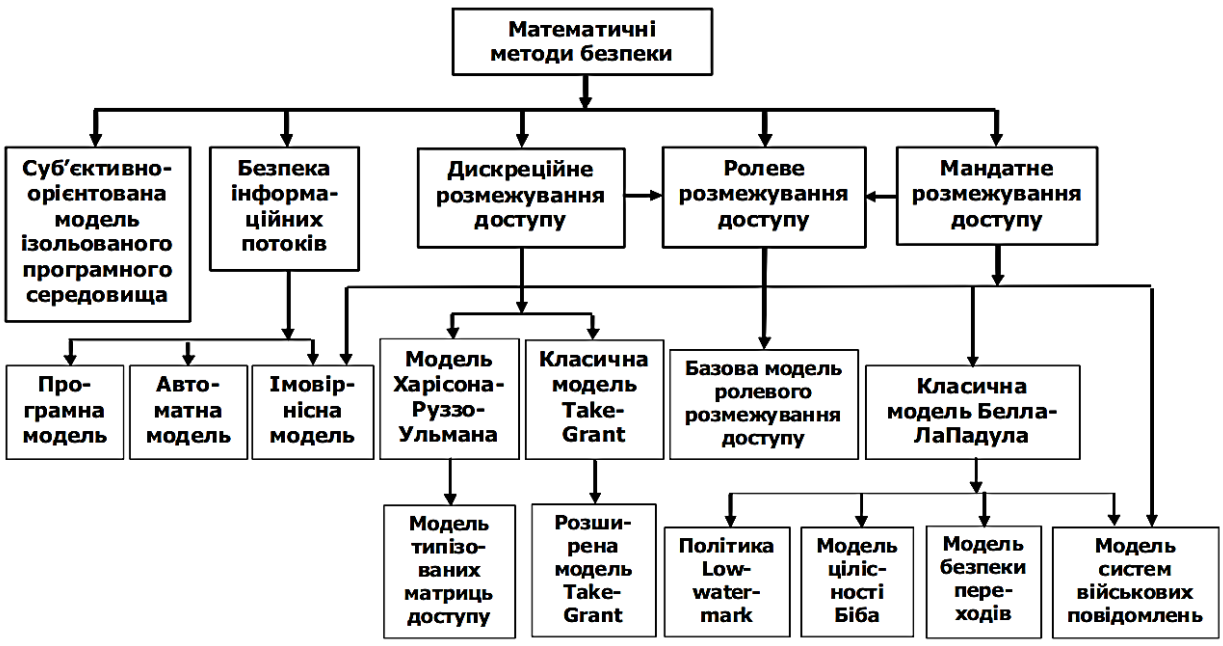


Рис. 1.5. Різновиди математичних моделей в галузі безпеки

Класифікація математичних моделей в галузі безпеки:

Використання математичних моделей для чіткого визначення політик безпеки, які визначають правила та обмеження для забезпечення конфіденційності та доступу до інформації. Наприклад, у формальному визначенні політики безпеки можна використовувати модель ролей та правил контролю доступу (RBAC). Тобто, визначаючи, що "Користувачі з роллю адміністратора мають право на повний доступ до всіх системних ресурсів."

Можна визначити політику безпеки конфіденційності, використовуючи математичні вирази. Наприклад, "Рівень конфіденційності даних (C) повинен бути більший за рівень користувача (U), щоб забезпечити доступ."

Формальне визначення політики безпеки може також стосуватися процесів ідентифікації. "Процедура ідентифікації має бути еквівалентною математичній функції, яка гарантує унікальність ідентифікаторів користувачів."

Можна визначити, що "Заборонено здійснювати запис на зовнішні пристрої без шифрування" як формальну політику безпеки для захисту даних.

Математичні моделі, що досліджують та обґрунтовують методи інформаційного захисту, включаючи шифрування, контроль доступу та ідентифікацію.

Теорія захисту інформації використовує математичні моделі для дослідження та розробки ефективних методів захисту конфіденційності, цілісності та доступу до інформації. Основні напрямки включають шифрування, контроль доступу, аутентифікацію та інші аспекти інформаційної безпеки.

В теорії захисту інформації, асиметричне шифрування використовує математичні моделі, такі як RSA (Rivest–Shamir–Adleman). У цій моделі використовуються математичні принципи теорії чисел, зокрема проблеми факторизації великих простих чисел, для створення пари ключів: публічного та приватного.

Користуючись математичними властивостями простих чисел, RSA створює ключі, де публічний ключ може бути розповсюджений, але лише власник приватного ключа може ефективно розшифрувати зашифровані повідомлення. Така математична модель гарантує безпеку шифрування.

Такий приклад ілюструє, як математичні моделі в теорії захисту інформації застосовуються для розробки шифрування та забезпечення конфіденційності інформації. Розробка математичних моделей, які визначають структуру та взаємодію елементів інформаційних систем для досягнення високого рівня безпеки.

Моделі безпеки інформаційних систем використовують математичні концепції для аналізу та дизайну безпечних структур та взаємодій компонентів інформаційних систем. Ці моделі спрямовані на досягнення високого рівня конфіденційності, цілісності та доступності даних.

Модель безпеки інформаційної системи, яка використовує одноразові паролі для аутентифікації, може базуватися на математичних принципах алгоритмів генерації OTP. Наприклад, алгоритм TOTP (Time-Based One-Time Password) базується на математичних обчисленнях з використанням ключа та поточного часу для генерації унікального пароля.

При використанні системи з одноразовим логуванням, математична модель TOTP гарантує, що кожен одноразовий пароль унікальний та може бути використаний лише протягом короткого періоду часу, що забезпечує високий рівень аутентифікації та конфіденційності.

Такий приклад ілюструє, як математичні моделі в багатофакторних системах безпеки інформаційних систем можуть гарантувати ефективні механізми захисту.

Використання математичних концепцій для розробки методів відновлення даних та забезпечення їх цілісності в умовах можливих порушень безпеки.

Створення математичних моделей, які точно визначають процеси аутентифікації та авторизації для ефективного контролю доступу до різних рівнів інформації.

Дослідження та моделювання різноманітних загроз та ризиків для розробки стратегій та методів мінімізації впливу можливих загроз на безпеку.

Математична теорія загроз дозволяє моделювати різноманітні загрози, їх ймовірності та потенційний вплив на інформаційну систему.

Баєсівська мережа – математична модель, що дозволяє визначити ймовірність виникнення загрози на основі взаємозв'язків між різними факторами. Наприклад,

модель може враховувати зв'язок між вразливістю програмного забезпечення та ймовірністю виникнення кібератаки.

Математична теорія ризиків дозволяє оцінити потенційний збиток чи втрату внаслідок конкретної загрози та визначити ймовірність цієї втрати.

Модель капіталовкладень – використовується для оцінки ризику в інвестиційному портфелі. Застосовується до визначення ймовірності різних фінансових сценаріїв та їх впливу на капіталовкладення.

Організація розглядає можливі загрози та ризики, пов'язані з впровадженням нової інформаційної системи.

Застосування баєсівської мережі для оцінки ймовірності кібератак та визначення зв'язку між вразливістю системи та потенційним впливом атаки.

Використання моделі капіталовкладень для розрахунку ризику фінансових втрат в разі успішної кібератаки та розробки стратегій мінімізації цього ризику.

Такі математичні моделі надають теоретичну базу для розробки та впровадження сучасних систем захисту інформації відповідно до вимог нормативних документів та стандартів.

1.4. Актуальні виклики інформаційної безпеки в сучасному контексті

Специфікація сучасних проблем інформаційної безпеки включає в себе широкий спектр викликів і труднощів, які стикаються організації та спеціалісти з інформаційної безпеки в сучасному світі. Розглянемо більш детально дані етапи:

- *Зростання обсягу та різноманітності загроз.* За останні роки спостерігається збільшення кількості та різноманітності кіберзагроз. Від зловмисного програмного забезпечення та фішингових атак до складних кібер-війн, організації повинні стежити за різноманітними загрозами та розробляти стратегії їхнього виявлення та запобігання.
- *Недостатня кількість кваліфікованих кадрів*. Інформаційна безпека вимагає високого рівня експертизи, і велика кількість організацій стикається з

проблемою нестачі кваліфікованих фахівців у цій галузі, що ставить під загрозу здатність ефективно захищати системи та дані.

- *Використання новітніх технологій*. Впровадження новітніх технологій, таких як хмарні сервіси, штучний інтелект, Інтернет речей тощо, відкриває нові можливості, але також створює нові вектори атак. Недостатня безпека цих технологій може призвести до серйозних наслідків для організацій.
- *Законодавчі та регуляторні вимоги*. Зростання вимог до захисту інформації, зокрема через введення нових законодавчих норм, таких як Загальний регламент з захисту даних (GDPR), ставить під високий тиск організації, які повинні відповідати цим стандартам та забезпечити відповідність.
- *Соціальна інженерія та людський фактор*. Зловмисники все частіше використовують соціальну інженерію, спрямовану на вплив на людей та отримання конфіденційної інформації. Людський фактор залишається однією з найбільш вразливих ланок в системі безпеки.
- *Неодноразові атаки на великі компанії*. Великі корпорації та організації є об'єктом постійних кібератак, і вони повинні постійно оновлювати свої заходи безпеки, щоб утримати криміналів та хакерів.
- *Комплексність систем і архітектур*. З більшою кількістю підключених пристроїв та складнішими інформаційними системами зростає складність захисту від потенційних атак.

У першому розділі «Аналіз специфікарів архітектурних рівнів для захисту інформації в мережі інтернету речей (IoT)» був проведений аналіз особливостей архітектурних рівнів для забезпечення безпеки інформації в мережі Інтернету речей (IoT). Розглянуті питання визначення актуальності проблеми захисту в IoT, опис архітектури IoT, математичні визначення безпеки систем, а також актуальні виклики інформаційної безпеки в сучасному контексті.

Першочергово, визначення актуальності проблеми захисту в IoT вказало на необхідність удосконалення систем безпеки в умовах стрімкого розвитку цієї галузі. Опис архітектури IoT розкрив важливі компоненти та взаємозв'язки між ними, що дозволяє краще розуміти особливості системи.

Математичні визначення безпеки систем стали фундаментальним елементом розділу, забезпечуючи теоретичну базу для подальших досліджень. Аналіз актуальних викликів інформаційної безпеки наголосив на постійно зростаючій складності та різноманіття загроз, що вимагає вдосконалення заходів захисту.

Отже, аналіз архітектурних рівнів для захисту інформації в мережі IoT надав важливий внесок у розуміння сучасних викликів і потреб у сфері безпеки цієї інноваційної галузі. Результати досліджень формують підґрунтя для подальшого розвитку ефективних стратегій та методів захисту інформації в мережі Інтернету речей.

РОЗДІЛ 2. АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ (IoT).

2.1 Апаратний захист інформації

Апаратний захист інформації – це один з видів захисту інформації, який реалізується на апаратному рівні. Апаратний захист інформації включає в себе такі засоби, як:

- Схеми контролю на чесність, які перевіряють правильність передачі інформації між різними пристроями. Схеми контролю на чесність – це апаратні засоби, які контролюють правильність передачі інформації між різними приладами ЕОМ. Схеми контролю на чесність використовуються для запобігання помилкам, що можуть виникнути через збої обладнання, перешкоди в каналах зв'язку, навмисні атаки тощо. Схеми контролю на чесність можуть бути реалізовані на різних рівнях: бітовому, символьному, блочному, пакетному тощо. Схеми контролю на чесність використовують різні методи для перевірки інформації, наприклад, парність, контрольні суми, циклічні коди, хеш-функції, цифрові підписи тощо.
- Екрануючі прилади, які локалізують електромагнітні випромінювання, що можуть створювати технічні канали витоку інформації. Екрануючі прилади – це прилади, які локалізують електромагнітні випромінювання, що можуть

створювати технічні канали витоку інформації. Екрануючі прилади використовуються для захисту інформації від несанкціонованого перехоплення або підриву. Екрануючі прилади можуть бути пасивними або активними. Пасивні екрануючі прилади створюють перешкоди для проникнення електромагнітних хвиль, наприклад, металеві оболонки, сітки, фольги тощо. Активні екрануючі прилади генерують власні електромагнітні поля, які нейтралізують або змінюють випромінювання джерела інформації, наприклад, шумові генератори, модулятори, перетворювачі тощо.

- Смарт-карти, токени, біометричні сканери, які забезпечують аутентифікацію і авторизацію користувачів. До технічних засобів захисту також належать біометричні методи, такі як зчитування візерунка сітчатки ока, відбитків пальців, геометрії рук, динаміки підпису.
- Криптографічні пристрої, які здійснюють шифрування і розшифрування інформації.

Апаратний захист інформації має свої переваги і недоліки. До переваг належать:

- Висока швидкість і надійність обробки інформації.
- Менша залежність від програмного забезпечення і людського фактору.
- Можливість захисту від фізичних впливів і навмисних пошкоджень.

До недоліків належать:

- Висока вартість і складність розробки і обслуговування.
- Обмежена сумісність і масштабованість.
- Необхідність дотримання спеціальних умов експлуатації і зберігання.

Крім того, існують комплекси технічних засобів захисту від несанкціонованого доступу, які можна розділити на наступні категорії:

- Захист від електромагнітного випромінювання включає в себе використання оптоволоконних кабелів, захисної плівки на вікнах та захищених дисплеїв, захист від поновлення знищених даних.
- Захист від підслуховування включає в себе встановлення фільтрів на лініях зв’язку, запобігання встановленню підслуховувальних пристроїв,

використання звукопоглинальних покриттів та проти підслуховувального зашумлення.

Для захисту інформації в мережах потрібні різні пристрої, залежно від типу мережі, рівня захисту, обсягу та швидкості передачі даних. Ось деякі приклади таких пристроїв:

Криптографічні пристрої (КП) – це пристрої, які виконують шифрування та розшифрування даних за допомогою симетричних або асиметричних алгоритмів. КП можуть бути вбудовані в апаратуру мережі або підключатися до неї через стандартний інтерфейс.

Криптографічні ключові системи (ККС) – це системи, які забезпечують генерацію, розподіл, зберігання та управління ключами шифрування, які використовуються КП. ККС можуть бути апаратними або програмними, централізованими або розподіленими.

Мережеві екрани (firewalls) – це пристрої, які контролюють вхідний та вихідний трафік мережі, фільтруючи його за допомогою правил доступу. Мережеві екрани можуть бути апаратними або програмними, периметральними або внутрішніми.

Мережевий екран, також відомий як фаєрвол (Firewall), це пристрій або набір пристроїв, які налаштовані для керування комп'ютерним трафіком між областями різної безпеки відповідно до встановлених правил та інших критеріїв. Фаєрвол може бути реалізований як окремий пристрій, наприклад, маршрутизатор або роутер, або як програмне забезпечення, встановлене на персональний комп'ютер чи проксі-сервер. Відомо, що існують три основні типи фаєрволів: мережевий рівень, прикладний рівень і рівень з'єднання.

Мережевий рівень (Network Layer) – фаєрвол, який виконує фільтрацію пакетів на рівні мережевого та транспортного рівнів моделі OSI. Він контролює лише дані службової інформації пакетів, залишаючи інші рівні неконтрольованими. Ці фаєрволи можуть бути менш гнучкими у налаштуванні та вразливими до деяких видів атак.

Прикладний рівень (Application Layer) – проксі-сервер, цей фаєрвол встановлює фізичний поділ між локальною мережею та Інтернетом, що надає йому високий рівень безпеки. Проте аналіз пакетів та впровадження контролю доступу можуть знизити продуктивність мережі.

Рівень з'єднання (Connection Level) – фаєрвол прикладного рівня, але обслуговує більшу кількість протоколів. Цей тип фаєрволів також використовується як сервер-посередник, забезпечуючи безпеку та ефективність мережі.

Вибір конкретного типу фаєрволу залежить від потреб користувача та вимог безпеки мережі.

Системи виявлення та запобігання вторгнень (IDS/IPS) – це системи, які аналізують трафік мережі, виявляючи та блокуючи аномальні або підозрілі дії, які можуть свідчити про атаки на мережу. IDS/IPS можуть бути апаратними або програмними, мережевими або хостовими.

VPN-пристрої (Virtual Private Network) – це пристрої, які дозволяють створювати захищені віртуальні мережі між різними локаціями, використовуючи загальнодоступні канали передачі даних, такі як Інтернет. VPN-пристрої використовують шифрування, аутентифікацію та тунелювання для забезпечення конфіденційності, цілісності та доступності даних.

VPN-пристрій працює в такому режимі, коли підключаєтеся до VPN-пристрою, він встановлює захищене з’єднання між вашим пристроєм та одним із його серверів, який знаходиться в іншій локації. Тоді інтернет-трафік проходить через це з’єднання, шифруючись та приховуючи реальну IP-адресу користувача. Видається, ніби заходить в інтернет з того сервера, до якого підключилися. VPN-пристрій використовує різні протоколи для шифрування та передачі даних, такі як PPTP, L2TP, SSTP, IKEv2, OpenVPN тощо. Ці протоколи визначають рівень безпеки, швидкості та сумісності VPN-пристрою з різними операційними системами та мережами. VPN-пристрій дозволяє отримати доступ до будь-якого контенту в інтернеті, обходячи геоблокування, цензуру та обмеження провайдерів. Також він захищає конфіденційність та особисті дані від сторонніх очей, особливо коли користуєтеся публічним Wi-Fi.

PPTP (англ. Point-to-Point Tunneling Protocol) – це тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі. PPTP використовує TCP-канал для керування тунелем і протокол Generic Routing Encapsulation для інкапсуляції PPP-пакетів. PPTP має багато відомих проблем з безпекою і вважається застарілим методом для реалізації віртуальних приватних мереж. PPTP був розроблений консорціумом вендорів, до якого входили Microsoft, Ascend Communications, 3Com та інші. PPTP підтримується більшістю операційних систем, але з версій macOS Sierra і iOS 10 він був видалений з міркувань безпеки. PPTP – це найстаріший і найшвидший протокол VPN, але також найменш безпечний. Він легко налаштовується на більшості пристроїв, але не рекомендується для захисту конфіденційної інформації.

L2TP (англ. Layer 2 Tunneling Protocol) – це протокол тунелювання, який використовується для підтримки віртуальних приватних мереж (VPN) або як частина надання послуг інтернет-провайдерами. Він використовує шифрування тільки для своїх власних керуючих повідомлень (за допомогою необов'язкового попередньо спільного секрету) і не забезпечує жодного шифрування або конфіденційності вмісту сам по собі. Замість цього, він надає тунель для рівня 2 (який може бути зашифрований), і сам тунель може бути переданий через протокол шифрування рівня, такий як IPsec. L2TP – це протокол, який використовується разом з IPSec для шифрування і аутентифікації даних. Він більш безпечний, ніж PPTP, але також більш повільний і може бути блокований деякими мережами. Він підтримується більшістю пристроїв, але потребує більше налаштувань.

L2TP був опублікований у серпні 1999 року як запропонований стандарт RFC 2661 і має своє походження переважно в двох старіших протоколах тунелювання для точка-точка зв'язку: Cisco's Layer 2 Forwarding Protocol (L2F) і Microsoft's Point-to-Point Tunneling Protocol (PPTP). Нова версія цього протоколу, L2TPv3, з'явилася як запропонований стандарт RFC 3931 у 2005 році. L2TPv3 надає додаткові функції безпеки, поліпшену інкапсуляцію і здатність переносити лінки даних, інші, ніж

просто Point-to-Point Protocol (PPP) через IP-мережу (наприклад, Frame Relay, Ethernet, ATM тощо).

SSTP (англ. Secure Socket Tunneling Protocol) - це протокол VPN, який створює тунель між клієнтським пристроєм і сервером. Він використовує SSL/TLS для шифрування і перевірки цілісності даних та був розроблений Microsoft, а також є дуже безпечним і здатним обходити брандмауери і проксі-сервери. Він головним чином підтримується Windows, але також доступний для деяких інших ОС123.

IKEv2 – це протокол, який також використовується разом з IPSec для шифрування і аутентифікації даних. Він дуже швидкий і стабільний, особливо для мобільних пристроїв, які часто змінюють мережі. Він підтримується Windows, macOS, iOS, Android і деякими іншими ОС.

OpenVPN – це сучасний і гнучкий протокол VPN, який використовує різні алгоритми шифрування для забезпечення високого рівня безпеки. Він також добре працює в умовах обмеженого доступу до мережі. Він не вбудований в жодну ОС, але підтримується більшістю VPN-клієнтів. Він вважається найкращим протоколом VPN для загального використання.

IDS/IPS-пристрої (Intrusion Detection System/Intrusion Prevention System) – це пристрої, які аналізують трафік мережі, виявляючи та блокуючи аномальні або підозрілі дії, які можуть свідчити про атаки на мережу. IDS/IPS-пристрої використовують сигнатури, аномалії, протоколи та інші методи для визначення загроз.

Антивірусні пристрої – це пристрої, які захищають комп'ютери та інші пристрої від вірусів, троянів, червів, шпигунського ПЗ та інших шкідливих програм. Антивірусні пристрої можуть бути вбудовані в мережеві пристрої, такі як маршрутизатори, комутатори, файрволи тощо, або підключатися до них через стандартний інтерфейс

Система виявлення атак (вторгнень) – це програмний чи апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу, або несанкціонованого управління ними, переважно через Інтернет. Ці системи, також відомі як IDS (Intrusion Detection System), надають

додатковий рівень безпеки комп’ютерних систем разом із системами запобігання вторгненням (IPS – Intrusion Prevention System). IDS можуть сповіщати про початок атак на мережу, деякі з них виявляють атаки, які раніше були невідомі. IPS не лише повідомляють про атаку, але і приймають рішення та вживають заходів, спрямованих на блокування атаки, таких як розрив з’єднання або виконання заданих адміністратором скриптів. На практиці, часто використовуються програмно-апаратні рішення, які об'єднують функціональність обох типів систем, такі об'єднані системи відомі як IDPS. Відмінність міжмережевого екрана в тому, що він обмежує надходження певних видів трафіку для запобігання вторгненням, але не виявляє вторгнень, що відбуваються всередині мережі. Натомість, IDS пропускає трафік, аналізуючи його і сигналізуючи про підозрілу активність. Для виявлення порушень безпеки IDS використовує евристичні правила та аналіз сигнатур відомих комп'ютерних атак.

2.2. Основні стаціонарні засоби захисту інформації

Вібросистема WNG-006 – комплект розроблено для створення завад для систем перехоплення інформації, що працюють за допомогою віброакустичного каналу витоку (рис.2.1). Збірка включає блок формування завади та датчики. Блок генерує електричний сигнал, який промодульований випадковим чином. Датчик трансформує цей електричний сигнал, переданий по кабелю від блока формування завади, у вібросигнал. Датчик твердо закріплюється на захищеній поверхні і покриває площі від 1 до 1,5 кв. м. Розміри датчика: циліндр діаметром 50 мм і висотою 10 мм. Живлення блока формування завади – мережеве, 220 В / 50 Гц.

Рис.2.1. Вібросистема WNG-006

Фільтр "Граніт-8" призначений для заборони витоку акустичної інформації через телефонну лінію у випадку покладеної трубки телефонного апарата (рис.2.2).

Основні технічні та експлуатаційні характеристики:

- Призначений для роботи на навантаженні 600 Ом +/-10 % в безперервному режимі.
- Загасання в діапазоні частот 0,15-10 кГц при вхідному сигналі рівнем 10 В не перевищує 3 дБ.
- Загасання при вхідній напрузі 10 В на частоті 50 Гц не менше 6 дБ, на частоті 100 кГц не менше 10 дБ.
- Габаритні розміри виробу не перевищують 95×60×25 мм.
- Вага фільтра не перевищує 0,2 кг.

Рис.2.2. Фільтр "Граніт-8"

Пристрій "Буран-2" розроблено для запобігання незаконному запису акустичної інформації за допомогою диктофонів та передачі інформації за допомогою радіомікрофонів в приміщенні (рис.2.3). Система приглушення здійснюється шляхом встановлення непомітної для людського слуху завади. Пристрій складається з трьох функціонально та конструктивно завершених модулів: генератора завадливого сигналу, антенного вузла і блока живлення. Усі ці вузли розташовані на шасі, вбудованому в алюмінієвий кейс.

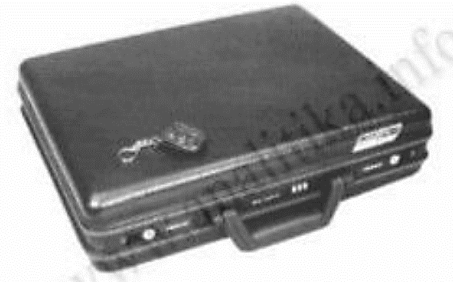


Рис.2.3. Виріб «Буран-2»

Основні технічні та експлуатаційні характеристики:

- Дальність приглушення – 1,5 метра.
- Ширина головного пелюстка на рівні 3 дБ – від 45 до 60 градусів.
- Напруга живлення від автономного джерела – від 30 до 32 Вольт.
- Споживаний струм від автономного джерела – менше 900 міліампер.
- Живлення – можливе від мережі 220 Вольт/50 Герц (а також від акумуляторів).

Рис.2.4. Диктофон PTKD-018

В стаціонарному цифровому виявнику диктофонів PTKD-018, що базується на мікропроцесорі 80C251 SB, використовуються передові принципи виявлення диктофонів, що дозволяють охопити до 16 посадкових місць (рис.2.4). При сприятливих умовах дальність виявлення складає 1,5 метра для кожного датчика. Системою можна управляти за допомогою комп'ютера, який підключається через порт RS-232, що надає можливість інтегрувати PTRD-018 у глобальну систему захисту.

Генератор "білого шуму" IVNG-022 призначений для ефективного захисту переговорів від систем промислового шпигунства та прослуховування (рис.2.5).

Прилад випромінює "білий шум" у головному спектрі звукових частот, що забезпечує маскування розмови і практично унеможливлює її розуміння після передачі через будь-які системи прослуховування. Генератор впливає безпосередньо на вхідні низькочастотні системи, такі як мікрофони, незалежно від їхньої схемотехніки та принципів передачі інформації.

Рис.2.5. Генератор шуму «Гном-3»

Генератор шуму "Гном-3" призначений для "маскування" корисної інформації, що міститься побічному електромагнітному випромінюванні. Основні технічні та експлуатаційні характеристики

Рівень шумового сигналу на вихідному роз'ємі генератора в діапазоні частот:

- від 10 до 150 кГц (f = 200 Гц) - менше 70 дБ;
- від 150 кГц до 30 МГц (f прийому = 9 кГц) - не більше 70 дБ
- від 30 до 400 МГц (f прийому = 120 кГц) - 75 дБ або краще;
- від 400 до 1ГГц(f прийому = 120 кГц) - 45 дБ або краще.

Ослаблення рівня сигналу в під діапазонах:

- від 10 до 150 кГц – 30 дБ або менше;
- від 150кГц до 30 МГц – 30 дБ або менше;
- від 30 до 300 МГц: 20 дБ і більше.

Коефіцієнт ентропійного шуму 0,8 або краще.

СТО-24 "Завірюха" – прилад призначений для контролю параметрів телефонної лінії.

Призначений для виявлення несанкціонованих гальванічних з'єднань електронних засобів збору даних (ЕЗЗД) і запобігання або усунення нормальної роботи цих пристроїв.

Перешкоджає нормальній роботі цих пристроїв та може бути модифіковане для роботи на АТС і має наступне:

1) придушувати послідовно з'єднані електронні охоронні пристрої з м'якими" каналами радіопередачі. "М'який" канал радіо передачі (без кристалічної стабілізації частоти) значно знижує потужність передачі (відношення сигнал/шум) паралельно з'єднаних ЗЗР з "жорсткими" каналами радіопередачі (кристалічною стабілізацією частоти);

2) зниження ефективності використання паралельно з'єднаних ЗЗР;

3) зниження ефективності використання паралельно з'єднаних ЗЗР з "м'якими" каналами шляхом зсуву/зміни спектру сигналу;

4) зниження ефективності використання паралельно з'єднаних ЗЗР з "м'якими" каналами шляхом зсуву/зміни спектру сигналу. Включення підслуховуючих пристроїв, керованих аудіосигналами, що передають і записують не інформацію, а шум.

При вимкненому телефоні:

- встановіть пасивні бар'єри проти прийому сигналів голосового діапазону з телефонних ліній за допомогою індуктивних датчиків;
- зменшити співвідношення сигнал/шум щонайменше втричі;
- встановлення пасивних бар'єрів для запобігання поширенню високочастотних сигналів несучої частоти радіопередавача на телефонну лінію;
- 0.15...15 кГц і забезпечують загасання при рівні вхідного сигналу не більше10 В;
- забезпечити загасання не більше 3дБ в смузі частот 0,15...15 кГц при рівні вхідного сигналу 10 В;
- забезпечення загасання – 50 кГц при рівні сигналу 10В.
  - 60 дБ і менше на частоті-100кГц;

- 100дБ і менше на частоті 100к Гц.

Основні технічні та експлуатаційні характеристики:

– живлення генератора завадових хвиль від телефонної лінії – 60В;
– струм споживання в захисному режимі – 500 мкА;
– живлення від батареї – 9 В;
– похибка вимірювання U ± 0,2;
– амплітуда прямокутного шумового сигналу від 4,5 до 5 В;
– розміри 12,5 × 68 × 40 мм.

Професійна багатодіапазонна радіостанція AR-3000A (рис.2.6), яка оснащена рідкокристалічним дисплеєм, на якому відображається рівень сигналу (дБ), частота прийнятого сигналу, метод модуляції, номер каналу пам'яті, режим роботи і т.д. та може використовуватися разом з IBM/PC.

Може використовуватися з IBM/PC за наявності від повідного програмного забезпечення. Дозволяє підключати магнітофон, динаміки, навушники, акустичну системи.

Рис.2.6. Радіоприймач AR-3000A

Основні технічні та експлуатаційні характеристики.

– діапазон частот 100 кГц – 2 036 МГц;
– види модуляції USB, LSB, CW, AM, NFM, WFM;
– кількість каналів пам'яті 4 банки (по 100 каналів);
– чутливість;
– аудіовихід 4-8 Ом;
– напруга 13,8 В (від мережі 110/220 В);
– розміри 138×80×200 мм.

Таблиця 2.1. Вид модуляції

Діапазон	Вид модуляції			
	SSB/C W	AM	NFM	WFM
1 Мгц - 2.5 Мгц	1.0 мВ	3.2 мкВ	–	–
2.5 мГц-1.8 ГГц	0.25 мкВ	1.0 мкВ	0.35 мкВ	1.0 мкВ
1.8 ГГц-2 ГГц	0.75 мкВ	1.0 мкВ	1.25 мкВ	3.0 мкВ

Портативний нелінійний радар"АТ-6" призначений для виявлення пристроїв, що містять напівпровідникові елементи, такі як транзистори, діоди та мікросхеми.

Основні технічні та експлуатаційні особливості:

- виріб сумісний як з джерелами живлення змінного струму частотою 50Гц і напругою 220 В, так із джерелами живлення постійного струму напругою 12 В;
- живлення блоку живлення здійснюється від джерела постійного струму напругою 12 В.

Споживана потужність джерела живлення наступна:

- не більше 4 Вт в імпульсному режимі;
- час безперервної роботи виробу – не більше 8 годин;
- вага портативного блоку нелінійної радіолокації не перевищує 2 кг;
- передавач працює в імпульсному режимі на частоті 905+1 МГц;
- тривалість імпульсу не більше1,5 мкс;
- частота повторення імпульсів;
- 400+50 Гц в імпульсному режимі;
- 20+1 кГц в огинаючому режимі;
- частота налаштування дорівнює подвоєній частоті передавача.
- реальна чутливість при співвідношенні сигнал/шум не менше 6 дБ, а при вихідній напрузі 0,1 В (амплітудне значення) – не гірше 10 – 11 дБ.

– регулювання посилення приймача здійснюється плавно в діапазоні 0 – 30 дБ.
– узагальнена ширина діаграми спрямованості за рівнем 0,5 не більше 90°.

2.3. Засоби та системи для виявлення, пошуку та нейтралізації технічних засобів, що вилучають інформацію.

Сучасне мережеве обладнання надає розширені можливості для обробки різноманітних видів трафіку. Однак пристрій може виконувати різні функції, такі як надання доступу до магістральної мережі, маршрутизація даних, інтеграція голосових програм, забезпечення високого рівня захисту інформації, передача відео в режимі реального часу і багато іншого. На ринку телекомунікацій представлені пристрої різних класів за продуктивністю та функціональними можливостями, від компактних для малих офісів до потужних для центральних офісів.

Для організації обміну інформацією між малими офісами та їх підключення до Інтернету рекомендуються компактні пристрої, які мають достатній функціонал для маршрутизації різних видів трафіку та деякі засоби захисту мережі. Для середніх офісів доступна лінійка обладнання з можливістю концентрації інформаційних потоків різного характеру, підключення до Інтернету, високорозвиненою системою безпеки та управління, а також підвищеною продуктивністю. Найвищими характеристиками, включаючи продуктивність, пропускну здатність, засоби захисту та управління, володіє обладнання для центральних офісів.

Однією з основних задач при побудові мережі є забезпечення керованості та захищеності мережі. Управління корпоративною мережею є неперервним процесом, спрямованим на забезпечення її надійної роботи. Проблеми, зазвичай, не виникають раптово, але, скоріше, виникають через некоректне використання ресурсів мережі, погіршення якості обслуговування або внесення змін в інфраструктуру мережі. Реагування на зміни у стані мережі важливо забезпечити завдяки надійній системі управління.

Ще одним ключовим аспектом при створенні корпоративної мережі є забезпечення її безпеки. Гарантована стійкість до зовнішніх впливів досягається шляхом прийняття єдиної політики безпеки та реалізації комплексу заходів для захисту інформації. Спеціалісти компанії повинні постійно слідкувати за дотриманням прийнятої політики безпеки та актуальністю її положень, оскільки нові технології можуть змінювати характер потоків даних в корпоративній мережі.

Мережевий захищений комплекс (МТК) розроблено для надійного обміну різними видами інформації, такими як дані, відео та аудіо, на високому рівні конфіденційності.

Комплектація МТК включає у себе мережеве обладнання, засоби криптографічного захисту інформації (шифратори), систему електроживлення та інші компонент (рис.2.7).

Рис.2.7. Схема використання

МТК може застосовуватися як на стаціонарних об'єктах, так і на рухомих. У ролі абонентського обладнання, яке може бути підключене до МТК (рис.2.8), можливе використання захищених комп'ютерів, IP-телефонів "Буковель", терміналів відеоконференцзв'язку, а також аналогових телефонів.

Рис.2.8. Мережевий захищений комплекс

Характеристики системи:

- інформаційний обмін всіма видами інформації здійснюється на основі протоколу IP, що гарантує високі показники гнучкості, масштабованості та легкості взаємодії з іншими вузлами та системами зв'язку;
- модульна конструкція системи дозволяє створювати вузли спеціального зв'язку різного призначення та використовувати різні транспортні бази;
- для взаємодії між територіально рознесеними МТК використовуються канали проводового, супутникового, радіорелейного та стільникового (3G, 4G) зв'язку;
- захист інформації здійснюється за допомогою технічних та криптографічних засобів, спрямованих на запобігання несанкціонованому доступу, порушенню цілісності та достовірності, а також перехопленню інформації у відкритих каналах зв'язку та витоку через технічні канали.

Технічні характеристики:

Інтерфейси:

- 100Base-FX: до 24 (з можливістю розширення до 48);
- 1000Base-SX: до 2 (з можливістю розширення до 4).

Система електроживлення:

- діапазон напруги: 10-36 В постійного струму;
- споживана потужність: не перевищує 400 Вт;
- безпека: відповідає стандарту ДСТУ 4113-2001;
- електромагнітна сумісність: захист від витоку ПЕМВН, відповідає ГОСТ 30334-95 (група 1).

Умови експлуатації:

- режим роботи: безперервний, цілодобовий;
- робоча температура: від -20°С до 60°С;
- температура зберігання: від -35°С до 80°С;
- вологість: не більше 95% при 25°С;
- конструкція: контейнер 19", від 8 U до 16 U;
- габаритні розміри: 531×860 від 460 до 850 мм (Ш×Д×В);
- вага: від 20 до 70 кг.

Механізм роботи МТК в системі можна описати так:

- МТК складається з двох основних компонентів: криптографічних пристроїв (КП) та криптографічних ключових систем (ККС).
- КП встановлюються на кінцевих точках мережі, де відбувається обмін інформацією між користувачами. КП здійснюють шифрування та розшифрування даних за допомогою симетричних алгоритмів, таких як AES, DES, 3DES, RC4 тощо.
- ККС відповідають за генерацію, розподіл, зберігання та управління ключами шифрування, які використовуються КП. ККС використовують асиметричні алгоритми, такі як RSA, DSA, ECDSA, Діффі-Хелмана, Ель-Гамаля тощо. Асиметричні алгоритми – це алгоритми криптографії, які використовують два різних ключі: один для шифрування, а інший для розшифрування даних. Вони також називаються криптосистемами з відкритим ключем, оскільки один з ключів може бути публічно відомим, а інший тримається в таємниці. Асиметричні алгоритми забезпечують високий рівень безпеки, але також потребують більше обчислювальних ресурсів, ніж симетричні алгоритми:

  RSA (Rivest-Shamir-Adleman) – це алгоритм, який використовує великі прості числа для генерації ключів і заснований на складності розкладання на множники. Він може використовуватися для шифрування, розшифрування, цифрового підпису і аутентифікації.

  DSA (англ. Digital Signature Algorithm) – це алгоритм, який використовує дискретне логарифмування для генерації ключів і заснований на складності

обчислення дискретних логарифмів. Він може використовуватися тільки для цифрового підпису і аутентифікації.

ECDSA (англ. Elliptic Curve Digital Signature Algorithm) – це алгоритм, який використовує еліптичні криві для генерації ключів і заснований на складності обчислення дискретних логарифмів на еліптичних кривих. Він може використовуватися для шифрування, розшифрування, цифрового підпису і аутентифікації.

Діффі-Хелмана – це алгоритм, який використовує дискретне логарифмування для обміну секретним ключем між двома сторонами по відкритому каналу. Може використовуватися тільки для встановлення спільного секрету і не для шифрування, розшифрування, цифрового підпису або аутентифікації.

Ель-Гамаля – це алгоритм, який використовує дискретне логарифмування для шифрування і розшифрування даних. Використовуватися також для цифрового підпису і аутентифікації.

– Ключі шифрування передаються від ККС до КП за допомогою спеціальних протоколів, таких як IKE, SSL, TLS, SSH тощо. При цьому використовується аутентифікація, шифрування та цифровий підпис для забезпечення конфіденційності, цілісності та невідмовності ключів.

IKE (англ. Internet Key Exchange) – це протокол, який використовується для встановлення безпечного з'єднання між двома сторонами за допомогою обміну ключами і шифрування даних. Він є частиною протоколу IPsec, який захищає трафік IP і має дві версії: IKEv1 і IKEv2.

SSL (англ. Secure Sockets Layer) – це протокол, який використовується для шифрування і аутентифікації даних, які передаються між веб-браузером і веб-сервером. Він використовує сертифікати для перевірки ідентичності сторін і алгоритми шифрування для захисту вмісту та був замінений TLS, але деякі люди все ще використовують термін SSL для позначення TLS.

TLS (англ. Transport Layer Security) – це протокол, який використовується для шифрування і аутентифікації даних, які передаються між двома додатками, які використовують TCP. Він є наступником SSL і покращує його безпеку і

гнучкість. Він використовує сертифікати для перевірки ідентичності сторін і алгоритми шифрування для захисту вмісту. Широко використовується для захисту веб-трафіку, електронної пошти, месенджерів і інших додатків.

SSH (англ. Secure Shell) – це протокол, який використовується для безпечного віддаленого доступу до інших комп'ютерів. Він використовує пари ключів для аутентифікації сторін і алгоритми шифрування для захисту даних. Дозволяє виконувати команди, копіювати файли, тунелювати інші протоколи через захищене з'єднання.

При обміні захищеною інформацією між КП використовуються протоколи IPsec, які включають такі компоненти:

- ESP (Encapsulating Security Payload) – протокол для шифрування та аутентифікації даних.
- AH (Authentication Header) – протокол для аутентифікації джерела та цілісності даних.

Ці протоколи можуть використовуватися окремо або разом, в залежності від потреб захисту. IPsec може працювати в двох режимах: транспортному та тунельному. У транспортному режимі IPsec захищає тільки вміст IP-пакета, а у тунельному режимі IPsec захищає весь IP-пакет, обгортаючи його в новий IP-заголовок.

МТК може підтримувати різні типи мереж, такі як проводові, бездротові, супутникові, мобільні тощо. МТК також може підтримувати різні протоколи мережевого, транспортного та застосункового рівня, такі як IPv4, IPv6, ARP, ICMP, DHCP, DNS, NTP, SNMP, TCP, UDP, SCTP, RTP, RTCP, HTTP, HTTPS, FTP, SSH, Telnet, SMTP, POP3, IMAP, SIP, H.323 тощо.

Різні типи мереж потрібні для різних цілей та сценаріїв використання. МТК підтримує такі типи мереж:

LAN (Local Area Network) – це мережа, яка з'єднує комп'ютери та інші пристрої в межах невеликої території, наприклад, в одному будинку, офісі, школі тощо. Переваги LAN: висока швидкість передачі даних, низька вартість, легкість

налаштування та адміністрування, можливість спільного використання ресурсів та програм.

MAN (Metropolitan Area Network) – це мережа, яка з'єднує комп'ютери та інші пристрої в межах одного міста або агломерації. Переваги MAN: велика площа покриття, висока пропускна здатність, можливість підключення до інших мереж, таких як LAN або WAN.

WAN (Wide Area Network) – це мережа, яка з'єднує комп'ютери та інші пристрої в межах країни або навіть світу. Переваги WAN: глобальне покриття, доступ до великої кількості інформації та послуг, можливість віддаленої роботи та навчання.

Персональні мережі (Personal Area Networks - PAN) – це мережі, які з'єднують пристрої в межах невеликої відстані, наприклад, в одній кімнаті. Переваги PAN: простота налаштування, низька вартість, можливість обміну даними між особистими пристроями.

Локальні мережі (Local Area Networks - LAN) – це мережі, які з'єднують комп'ютери та інші пристрої в межах невеликої території, наприклад, в одному будинку, офісі, школі тощо. Переваги LAN: висока швидкість передачі даних, низька вартість, легкість налаштування та адміністрування, можливість спільного використання ресурсів та програм.

Кампусні мережі (Campus Area Network) – це мережі, які з'єднують комп'ютери та інші пристрої в межах одного міста або агломерації. Переваги MAN: велика площа покриття, висока пропускна здатність, можливість підключення до інших мереж, таких як LAN або WAN.

Глобальні мережі (Wide Area Networks - WAN) – це мережі, які з'єднують комп'ютери та інші пристрої в межах країни або навіть світу. Переваги WAN: глобальне покриття, доступ до великої кількості інформації та послуг, можливість віддаленої роботи та навчання.

МТК може підтримувати різні типи мереж, тому що він використовує універсальні протоколи IPsec та IKE, які можуть працювати з різними каналами передавання даних, такими як кабельні або бездротові. МТК також може адаптуватися до різних топологій мереж, таких як зірка, кільце, шина, дерево тощо.

2.4. Система захисту інформації з використанням криптографічних засобів.

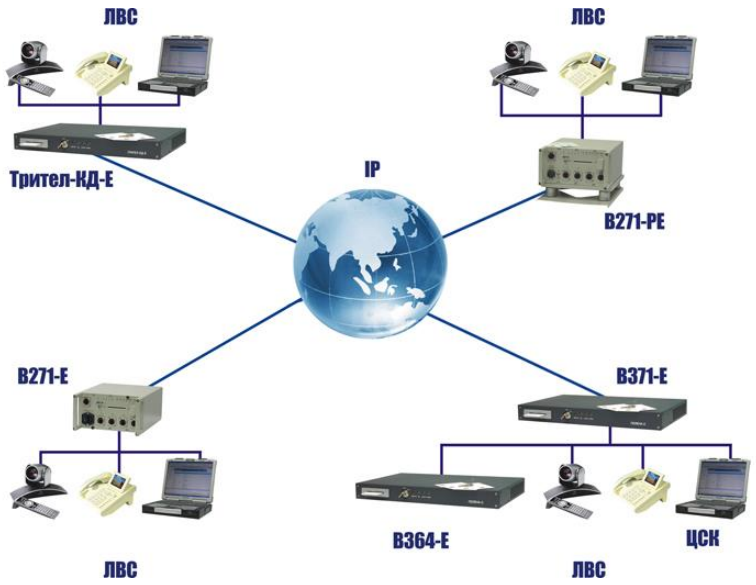


Рис. 2.9. Схема роботи криптографічного комплексу.

Криптографічний комплекс захисту інформації (рис.2.9):

- Шифратор В371-Е застосовується для захисту трафіку IP-мереж середнього рівня таємності в проводових, супутникових, радіорелейних та стільникових (3G, 4G) каналах зв'язку на стаціонарних об'єктах.
- Пристрій генерації ключових даних В364-Е використовується для генерації, зберігання та розподілу ключових даних.
- Централізована система керування (ЦСК) призначена для віддаленого управління мережею шифрованого зв'язку.

Функціональні характеристики:

Шифрування трафіку IP-мереж відбувається в периметрі локальної мережі, забезпечуючи "прозору" роботу мережевих додатків, обробку даних, IP-телефонію та відеоконференції у режимі on-line.

Під час обміну шифрованою інформацією створюються віртуальні канали шифрованого зв'язку, які задаються адміністратором комплексу.

Для кожного спрямування зв’язку можуть бути визначені декілька віртуальних каналів з різними маршрутами, що забезпечує резервування каналів зв’язку.

Централізована ключова система забезпечує генерацію та розподілення ключових даних за допомогою фізичних сенсорів, що відповідають FIPS 140-2. Розподілення може відбуватися через мережу шифрованого зв’язку або на носіях ключових даних.

Функції криптографічного перетворення реалізуються спеціалізованими мікросхемами з дублюванням, забезпечуючи високу пропускну здатність та надійність шифрування.

Комутація трафіку IP-мереж між різними каналами зв’язку, вибираючи оптимальний маршрут для кожного пакета.

Балансування навантаження та збільшення пропускної здатності вузлів мережі шляхом об’єднання віртуальних каналів шифрованого зв’язку в групи.

Обладнання дублюється для "гарячого" резервування та агрегування пропускної здатності.

Фільтрація трафіку за допомогою правил доступу, які визначають, які IP-адреси та порти можуть бути використані для обміну шифрованою інформацією.

Підтримка різних протоколів мережевого рівня, таких як IPv4, IPv6, ARP, ICMP, DHCP, DNS, NTP, SNMP.

Підтримка різних протоколів транспортного рівня, таких як TCP, UDP, SCTP, RTP, RTCP.

Підтримка різних протоколів застосункового рівня, таких як HTTP, HTTPS, FTP, SSH, Telnet, SMTP, POP3, IMAP, SIP, H.323

Моніторинг та керування обладнанням виконується локально та віддалено через централізовану систему керування (ЦСК). Програмне забезпечення ЦСК дозволяє керувати режимами роботи, змінювати параметри конфігурації, переглядати статистичну інформацію та обробляти події в мережі шифрованого зв’язку з захистом від несанкціонованого доступу через двофакторну аутентифікацію.

Механізм роботи шифратора В371-Е можна описати так:

Шифратор В371-Е отримує IP-пакети від мережевих пристроїв, які підключені до його портів, та визначає, чи потрібно їх захищати за допомогою IPsec.

Якщо IP-пакет потребує захисту, шифратор В371-Е перевіряє, чи існує віртуальний канал шифрованого зв'язку для цього напрямку. Якщо так, то шифратор В371-Е використовує ключі та параметри безпеки, які були попередньо встановлені за допомогою протоколу IKE.

Якщо віртуальний канал не існує, то шифратор В371-Е ініціює процес установки ключів та параметрів безпеки з відповідним шифратором на іншому кінці каналу. Для цього використовується протокол IKE, який складається з двох фаз:

На першій фазі шифратори обмінюються своїми сертифікатами та встановлюють захищене з'єднання, яке називається IKE SA (Security Association).

На другій фазі шифратори обговорюють ключі та параметри безпеки для віртуального каналу, який називається IPsec SA (Security Association).

Після того, як ключі та параметри безпеки встановлені, шифратор В371-Е застосовує до IP-пакета відповідні протоколи IPsec: ESP та/або AH. Це може включати шифрування, аутентифікацію, додавання нового IP-заголовка тощо .

Шифратор В371-Е передає захищений IP-пакет до комутатора, який вибирає оптимальний канал зв'язку для його доставки до одержувача .

Шифратор В371-Е також отримує захищені IP-пакети від комутатора, які прийшли з інших каналів зв'язку, та виконує зворотні процеси: перевіряє відповідність ключів та параметрів безпеки, розшифровує, перевіряє аутентифікацію, видаляє додатковий IP-заголовок тощо .

Шифратор В371-Е (рис. 2.10) передає розшифровані IP-пакети до мережевих пристроїв, які підключені до його портів, та забезпечує "прозору" роботу мережевих додатків.

Технічні характеристики:

Платформа використовує RISC архітектуру з процесором Freescale Power QUICC II™. Операційна система базується на RTOS - Triton OS™. У пристрої реалізовані різні протоколи, включаючи IP v.4, IP Multicast, DHCP client, та HSRP, з використанням криптографічних функцій, реалізованих апаратно, за принципом прохідного пакетного шифрування за стандартом ДСТУ ГОСТ 28147:2009.

Рис.2.10. Комплекс криптографічного захисту інформації Пелена-Е

Система має пропускну здатність до 70 Мб/с та сумісна з іншим обладнанням, зокрема В271-Е(РЕ). Забезпечено різні схеми зв'язку, такі як повнозв'язна, за напрямками, циркулярна та змішана.

Керування відбувається за допомогою Vt100 терміналу та централізованої системи керування (ЦСК). Фізичні інтерфейси включають 1 порт 100Base-TX для зовнішньої мережі, 1 порт 100Base-TX для локальної мережі, RS-232 для термінала керування та інтерфейс ISO-7816-2, 3 для введення ключових даних.

Електроживлення забезпечується системами В371-Е та В364-Е з діапазоном напруги 170-240 В та частотою 50-60 Гц. Споживана потужність не перевищує 40 Вт. Відповідно до стандартів ДСТУ 4113-2001, пристрій забезпечує безпеку інформації.

Пристрій розрахований на безперервний, цілодобовий режим роботи. Робоча температура від 0°С до 50°С, температура зберігання від -35°С до 80°С, а вологість не повинна перевищувати 95% при 25°С. Конструкція пристрою має форм-фактор 1U з можливістю монтажу в стандартну 19"-стійку. Габаритні розміри складають 430×257×51 мм, а вага становить 3,8 кг.

Криптографічний комплекс захисту інформації Пелена-Е може використовуватися для захисту інформації в різних сферах, таких як:

- Державне управління, де необхідно забезпечити конфіденційність, цілісність, автентичність та невідмовність документів, даних, комунікацій та послуг.
- Банківська та фінансова сфера, де необхідно захищати від витоку, зміни та підробки фінансової інформації, платіжних документів, електронних грошей, банківських карток, ідентифікаційних кодів тощо.
- Військова та оборонна сфера, де необхідно захищати від розвідки, перехоплення, збою та знищення військової інформації, команд, сигналів, зв'язку, навігації, радіолокації тощо.
- Наукова та освітня сфера, де необхідно захищати від крадіжки, плагіату, фальсифікації наукової інформації, дослідних даних, публікацій, патентів, дипломів, сертифікатів тощо.
- Медична та охоронна сфера, де необхідно захищати від порушення медичної таємниці, втрати, зміни, підробки медичної інформації, діагнозів, рецептів, аналізів, карток, страхових полісів тощо.

Лавина-Е - це комплекс криптографічного захисту, який розробила українська компанія Tritel. Цей комплекс призначений для захисту трафіку IP-мереж високого рівня таємності від несанкціонованого доступу. Комплекс складається з трьох основних компонентів: шифратора О371-Е (РЕ), пристрою генерації ключових даних О372-Е та централізованої системи керування (ЦСК). Шифратор О371-Е (РЕ) використовується для шифрування та розшифрування даних, які передаються по різних типах каналів зв'язку, таких як проводовий, супутниковий, радіорелейний або стільниковий. Пристрій генерації ключових даних О372-Е забезпечує генерацію, зберігання та розподіл ключів, які використовуються для шифрування. Централізована система керування (ЦСК) дозволяє віддалено керувати мережею шифрованого зв'язку, змінювати параметри конфігурації, переглядати статистику та протоколи подій.

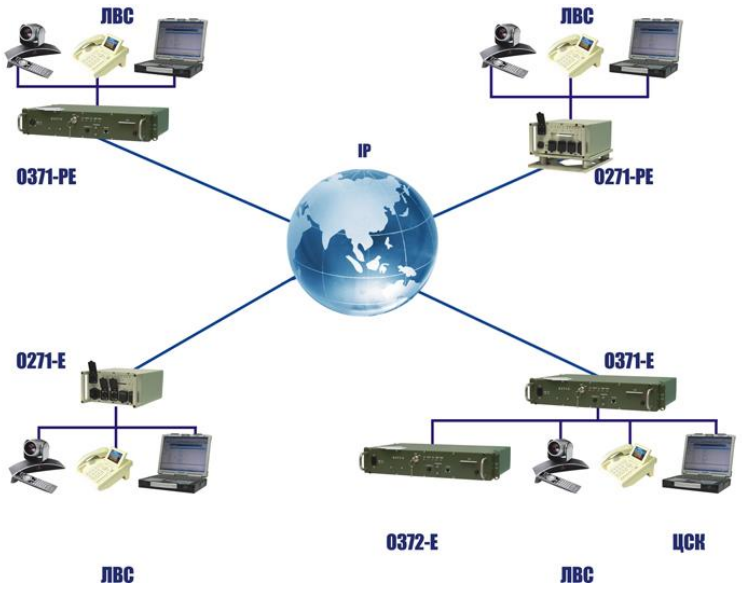


Рис.2.11. Схема застосування *Лавина-Е*

Лавина-Е працює на основі пакетного, прохідного шифрування, яке здійснюється спеціалізованими мікросхемами з дублюванням (рис.2.11). Алгоритм шифрування, який використовується, є ДСТУ ГОСТ 28147:2009, який є українською адаптацією російського стандарту ГОСТ 28147-89. Цей алгоритм є симетричним блоковим шифром з довжиною блоку 64 біти та довжиною ключа 256 біт. Шифратор О371-Е (РЕ) може працювати у двох режимах: режимі гамування та режимі зворотного зв'язку за шифротекстом. Режим гамування полягає в тому, що кожен блок відкритого тексту додається по модулю 2 з відповідним блоком гамми, яка генерується з ключа. Режим зворотного зв'язку за шифротекстом полягає в тому, що кожен блок відкритого тексту додається по модулю 2 з попереднім блоком шифротексту, який потім шифрується з ключем. Ці режими забезпечують високу стійкість до лінійного та диференціального криптоаналізу. Для криптоаналізу Лавина-Е потрібно мати доступ до великої кількості пар відкритого тексту та шифротексту, а також знати структуру та параметри алгоритму шифрування. Якщо ж ключ змінюється часто, то криптоаналіз стає ще складнішим.

Платформа використовує архітектуру RISC з процесором Freescale Power QUICC II™. Операційна система базується на RTOS та Triton OS™. Підтримуються різні протоколи, такі як IP v.4 згідно з RFC 791, RFC 826, RFC 1042, RFC 1812, IP

Multicast згідно з RFC 3171, DHCP client згідно з RFC 2131, та HSRP згідно з RFC 2281.

Криптографічні функції реалізовані апаратно, використовується пакетний та прохідний принцип шифрування. Застосовується алгоритм шифрування згідно з ДСТУ ГОСТ 28147:2009 з пропускною здатністю до 70 Мб/с. Сумісність з О271-Е(РЕ), О171-Е.

Система має різні схеми зв'язку, включаючи повнозв'язну, за напрямками, циркулярну та змішану. Управління здійснюється через термінал Vt100, telnet, та ЦСК.

Фізичні інтерфейси включають 1 порт 100 Base-FX для зовнішньої мережі та 1 порт 100 Base-FX для локальної мережі, RS-232, RJ-45 для терміналу керування, ISO-7816-2, 3 для введення ключових даних.

Система електроживлення може бути О371-Е, О372-Е з напругою 170-240 В та частотою 50-60 Гц або О371-РЕ з напругою 10-36 В постійного струму і споживаною потужністю не більше 50 Вт.

Забезпечено безпеку згідно з ДСТУ 4113-2001 та електромагнітну сумісність від витоку ПЕМВН згідно з ГОСТ 30334-95 (група 1).

Умови експлуатації передбачають безперервний режим роботи цілодобово. Робоча температура може коливатися від 0°С до 50°С для О371-Е, О372-Е, та від -20°С до 60°С для О271-РЕ. Температура зберігання від -35°С до 80°С, а вологість не повинна перевищувати 95% при 25°С.

Конструкція системи включає 3U з можливістю монтажу у 19"-стійку. Габаритні розміри становлять 482×345×106 мм (Ш×Д×В), а вага системи складає 8 кг.

Телекомунікаційна та інформаційна сфера, де необхідно захищати від незаконного доступу, перехоплення, збою, блокування телекомунікаційної та інформаційної інфраструктури, послуг, даних, голосу, відео, зображень тощо.

2.5. Бездротові мережі передачі даних

Бездротова мережа – це форма комп'ютерної мережі, де передача даних та з'єднання між мережевими вузлами відбувається за допомогою бездротового з'єднання (рис.2.12).

Рис.2.12. Wireless LAN (WLAN)

Бездротова локальна мережа (WLAN) - це форма мережі, де передача даних здійснюється через радіосигнали, а об'єднання пристроїв у мережу відбувається без використання кабельних з'єднань. Способи побудови WLAN включають Wi-Fi і WiMAX. Забезпечення безпеки в бездротових мережах залишається актуальною задачею, і технології, такі як WPA, використовуються для підвищення рівня безпеки під час під'єднання клієнтів до WLAN шляхом проходження процесу автентифікації.

Переваги:

- Здатність обслуговувати велику кількість пристроїв.
- Просте налаштування бездротової мережі, особливо у порівнянні з прокладанням дротових кабелів.
- Зручний доступ до WLAN у порівнянні з дротовою ЛВС, оскільки довжина кабелю не є фактором.
- Можливість розгортання бездротових локальних мереж навіть віддалено від бізнесу чи будинку, наприклад, у громадських приміщеннях.

Недоліки:

- Вища вразливість WLAN до зламу, тому необхідне ефективне шифрування.
- Можливість впливу бездротових перешкод на швидкість і стабільність мережі.
- Розширення бездротової мережі може вимагати додаткових бездротових пристроїв, таких як ретранслятори.
- Безсумнівно, є переваги в бездротових локальних мережах, але важливо не пропускати можливі проблеми.

Мережі WLAN можуть включати від двох до сотень і більше пристроїв. Проте збільшення кількості пристроїв у бездротових мережах робить їх управління складнішим завданням.

В бездротових локальних мережах можуть бути підключені різноманітні типи пристроїв, такі як мобільні телефони, ноутбуки, планшети, аудіосистеми для інтернету, ігрові приставки та інші пристрої, які мають підключення до Інтернету.

Обладнання та з'єднання в бездротових локальних мережах працюють за допомогою радіопередавачів і приймачів, вбудованих у клієнтські пристрої. Ці мережі не вимагають використання кабелів, але для їх розгортання зазвичай використовують різні спеціалізовані пристрої з власними радіоприймачами та антенами.

Локальні мережі Wi-Fi можуть бути побудовані в двох режимах: "спеціальному" та "інфраструктурному". Спеціальні мережі складаються з однорангових прямих з'єднань між клієнтами, без використання проміжних апаратних компонентів. Даний тип мережі може бути корисним для тимчасових зв'язків, але не завжди підходить для обслуговування багатьох пристроїв та може становити загрозу безпеці. Інфраструктурний режим використовує точку бездротового доступу (AP) для підключення всіх клієнтів. У домашніх мережах цю функцію може виконувати бездротовий маршрутизатор, що надає доступ до Інтернету. Можна об'єднати кілька точок доступу і створити мережі більшого масштабу.

2.6. Технології роботи Інтернет речей

Технології, такі як Wi-Fi, Bluetooth, LoRaWAN, NB-IoT, 5G. Це різні бездротові протоколи, які використовуються для зв'язку між пристроями Інтернету речей (IoT). Вони мають різні характеристики, переваги та недоліки, залежно від сценаріїв застосування. Ось деякі основні відмінності між ними:

Wi-Fi – це найпоширеніший протокол бездротового зв'язку, який використовується для підключення пристроїв до Інтернету через локальну бездротову мережу (WLAN). Wi-Fi пропонує високу швидкість передачі даних (до 10 Гбіт/с), велику пропускну здатність та низьку затримку, але має обмежений радіус дії (до 100 м) та високе енергоспоживання. Wi-Fi підходить для домашніх, офісних та громадських мереж, де потрібна висока якість зв'язку та доступ до Інтернету.

Bluetooth – це протокол бездротового зв'язку, який використовується для підключення пристроїв на невеликій відстані (до 10 м) за допомогою радіочастот (RF). Bluetooth пропонує низьку швидкість передачі даних (до 3 Мбіт/с), низьку пропускну здатність та низьке енергоспоживання. Bluetooth підходить для персональних мереж, де потрібна проста та енергоефективна комунікація між пристроями, такими як навушники, клавіатури, миші, годинники тощо.

LoRaWAN – це протокол бездротового зв'язку, який використовується для підключення пристроїв на великій відстані (до 15 км) за допомогою низькошвидкісних радіочастот (LF). LoRaWAN пропонує дуже низьку швидкість передачі даних (до 50 Кбіт/с), низьку пропускну здатність та дуже низьке енергоспоживання. LoRaWAN підходить для широкомасштабних мереж, де потрібна довготривала та надійна комунікація між пристроями, такими як сенсори, лічильники, трекери тощо.

NB-IoT – це протокол бездротового зв'язку, який використовується для підключення пристроїв на великій відстані (до 40 км) за допомогою вузькосмугових радіочастот (NB). NB-IoT пропонує низьку швидкість передачі даних (до 250 Кбіт/с), низьку пропускну здатність та низьке енергоспоживання. NB-IoT підходить для масових мереж, де потрібна проста та економічна комунікація між пристроями, такими як смарт-місто, смарт-сільське господарство, смарт-метрологія тощо.

5G – це нове покоління бездротового зв’язку, яке використовується для підключення пристроїв до Інтернету через мобільну мережу. 5G пропонує надвисоку швидкість передачі даних (до 20 Гбіт/с), високу пропускну здатність та наднизьку затримку, але має високе енергоспоживання та вимагає високої щільності базових станцій. 5G підходить для майбутніх мереж, де потрібна висока якість зв’язку та доступ до Інтернету для різних застосунків, таких як доповнена реальність, віртуальна реальність, автономні транспортні засоби, телемедицина тощо.

Другий розділ «*Апаратне забезпечення безпечної системи інтернету речей (IoT)*» присвячений апаратному забезпеченню системи Інтернету речей (IoT), де розглянуто різноманітні аспекти безпеки та захисту інформації. На основі досліджень пропонуються рішення та технічні засоби для забезпечення ефективного функціонування та захисту системи IoT. Основні аспекти розділу включають апаратний захист інформації, стаціонарні засоби захисту, системи для виявлення та нейтралізації технічних засобів, що вилучають інформацію, використання криптографічних засобів у системах захисту інформації та аспекти безпеки бездротових мереж передачі даних та на необхідність комплексного підходу до апаратного захисту Інтернету речей, оскільки відмічається постійний розвиток технологій та зростання загроз кібербезпеці. Розглядаються різноманітні засоби та системи, які сприяють виявленню та нейтралізації потенційних загроз, а також підкреслюється важливість використання криптографічних методів для захисту інформації. Бездротові мережі передачі даних визначаються як ключовий елемент, вимагаючи особливої уваги до їхньої безпеки.

Отже, другий розділ надає глибокий огляд апаратного забезпечення для Інтернету речей та визначає ключові аспекти безпеки та захисту інформації, враховуючи актуальні виклики та загрози в цьому сегменті технологій.

РОЗДІЛ 3. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ (IoT).

3.1. Визначення завдань для проєктування системи Інтернету речей (IoT).

При розробці мережі Інтернету речей необхідно враховувати два аспекти:

– фізичне планування мережі;

– логічне планування мережі.

Фізичне планування мережі включає в себе розгляд пристроїв IoT та використання протоколів. Існує ряд протоколів на різних рівнях, які забезпечують ефективне управління та взаємодію між пристроями IoT та серверами через Інтернет (рис. 3.1-3.5).

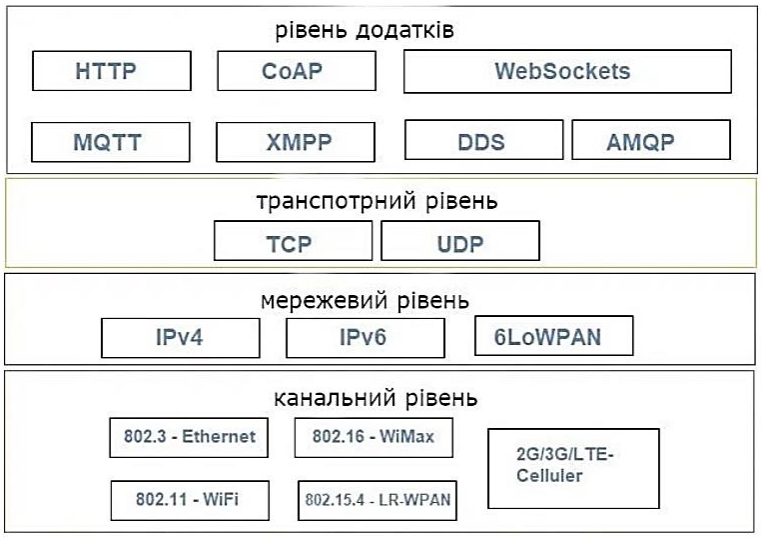


Рис.3.1. Протоколи для зв'язку в Інтернеті Речей

Протоколи *канального рівня* в мережі Інтернету речей (IoT) відіграють важливу роль у забезпеченні ефективного та безпечного обміну даними між пристроями. Найбільш поширеними протоколами на цьому рівні є:

IEEE 802.15.4 – це стандарт для бездротових особистих мереж, який визначає фізичний та канальний рівні. Використовується для створення низькорівневих мереж з невеликою витратою енергії, таких як Zigbee.

Zigbee – безпровідний протокол, побудований на основі стандарту IEEE 802.15.4. Використовується для забезпечення комунікації між простими та обмеженими ресурсами пристроями в мережах IoT.

Протоколи *мережевого рівня* визначають, як дані передаються між різними пристроями в мережі. Ось деякі з найвідоміших протоколів мережевого рівня:

IP (Internet Protocol) є основою для передачі даних в Інтернеті. Версія IP може бути IPv4 або IPv6. IPv4 використовує 32-бітні адреси, тоді як IPv6 використовує 128-бітні адреси, щоб забезпечити велику кількість можливих адрес.

ICMP (Internet Control Message Protocol) використовується для відправки повідомлень про помилки та іншої інформації про стан мережі. Найвідоміший приклад - команда "ping", яка використовує ICMP для визначення доступності пристрою в мережі.

IGMP (Internet Group Management Protocol) використовується для управління мультикастовими групами в мережі, що дозволяє пристроям приєднуватися до чи залишати мультикастові групи.

OSPF (Open Shortest Path First) – це протокол маршрутизації, який визначає найкоротший шлях для передачі даних в мережі, використовуючи алгоритм Дейкстри.

BGP (Border Gateway Protocol) використовується для обміну маршрутами між різними автономними системами у Інтернеті. Це особливо важливо для великих провайдерів мережевих послуг.

RIP (Routing Information Protocol) – простий протокол маршрутизації, який використовує алгоритм з обмеженим вектором для визначення найкоротших шляхів у мережі.

IPsec (Internet Protocol Security) забезпечує механізми безпеки для IP-трафіку, включаючи шифрування та автентифікацію, щоб захистити дані від несанкціонованого доступу.

Bluetooth Low Energy (BLE), а також відомий як Bluetooth Smart, даний протокол спрямований на забезпечення низького споживання енергії та високої ефективності в обміні даними, що робить його популярним для IoT-пристроїв.

LoRa (Long Range) – технологія для створення бездротових мереж з великим зондом покриття та низькою витратою енергії. Зазвичай використовується для великомасштабних IoT-застосувань, таких як сільське господарство або міське управління.

NFC (Near Field Communication) використовується для короткодистанційного обміну даними (зазвичай до 10 см). Застосовується в різних IoT-сценаріях, включаючи смарт-метри та безконтактні платежі.

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) протокол дозволяє передавати пакети IPv6 через мережі з обмеженими ресурсами, такі як Zigbee чи IEEE 802.15.4.

Thread розроблений для високофункціональних IoT-мереж, Thread використовує IPv6 і забезпечує надійний обмін даними у великих мережах.

RFID (Radio-Frequency Identification) протокол використовується для ідентифікації та взаємодії з об'єктами за допомогою радіочастотних міток. Застосовується у таких галузях, як логістика та управління запасами.

NB-IoT (Narrowband IoT) використовує мережі зв'язку для передачі невеликих обсягів даних в мережах з високою густотою пристроїв.

Weightless сімейство протоколів, спрямованих на машинне навчання та інші високопродуктивні застосування в IoT.

Протоколи *мережевого рівня* визначають, як дані передаються між різними пристроями в мережі. Ось деякі з найвідоміших протоколів мережевого рівня:

IP (Internet Protocol) є основою для передачі даних в Інтернеті. Версія IP може бути IPv4 або IPv6. IPv4 використовує 32-бітні адреси, тоді як IPv6 використовує 128-бітні адреси, щоб забезпечити велику кількість можливих адрес.

DHCP (Dynamic Host Configuration Protocol) використовується для автоматичного надання IP-адрес та інших конфігураційних параметрів пристроям в мережі.

ARP (Address Resolution Protocol) вирішує відповідність між IP-адресами та фізичними MAC-адресами в локальній мережі.

IPv6 Neighbor Discovery (ND) протокол використовується в IPv6 для виявлення сусідніх пристроїв в мережі та надання інформації про них.

PIM (Protocol Independent Multicast) дозволяє ефективно використовувати мультикастовий трафік в мережі, що особливо важливо для передачі даних на велику кількість пристроїв.

IP/MPLS (Multiprotocol Label Switching) комбінує маршрутизацію IP та перенаправлення на основі міток для оптимізації трафіку в мережі.

ICMPv6 (Internet Control Message Protocol version 6) варіант для IPv6, який надає повідомлення про стан та помилки в IPv6 мережах.

NDP (Neighbor Discovery Protocol) використовується в IPv6 для виявлення сусідніх пристроїв та обміну інформацією про них.

Протоколи *транспортного рівня* виконують ключові завдання у забезпеченні передачі даних між пристроями в мережі, забезпечуючи надійність і контроль цілісності. Розглянемо кілька важливих протоколів транспортного рівня:

TCP (Transmission Control Protocol) є одним з основних протоколів транспортного рівня. Він забезпечує надійний, послідовний та контрольований обмін даними між пристроями. TCP використовує механізми, такі як підтвердження та перевірка суми контрольної суми, для забезпечення доставки даних без помилок.

UDP (User Datagram Protocol) є іншим протоколом транспортного рівня, але він працює у режимі ненадійної доставки. Він швидший, ніж TCP, але не гарантує послідовності та доставки без помилок. UDP широко використовується для передачі даних в реальному часі, таких як відео- та аудіопотоки.

SCTP (Stream Control Transmission Protocol) протокол, який комбінує переваги як TCP, так і UDP. Він забезпечує надійну та послідовну доставку даних, але дозволяє використовувати кілька потоків для розділення різних видів даних.

QUIC (Quick UDP Internet Connections) протокол, розроблений компанією Google, який об'єднує переваги UDP та можливості керування з'єднанням, характерні для TCP. Він спроєктований для прискорення передачі даних в онлайн-середовищах та забезпечення безпеки.

CoAP (Constrained Application Protocol) протокол, спеціально розроблений для обмежених пристроїв та мереж Інтернету речей. Використовується для обміну даними між такими пристроями та забезпечення ефективності ресурсів.

MQTT (Message Queuing Telemetry Transport) протоколом для передачі повідомлень між пристроями в режимі реального часу. Забезпечує легкість використання та низький рівень бітового завантаження, що робить його популярним у мережах Інтернету речей.

Протоколи *рівня додатків* в мережах Інтернету речей (IoT) використовуються для взаємодії та обміну даними між різнорідними пристроями та системами. Ось декілька таких протоколів:

HTTP (Hypertext Transfer Protocol) є стандартним протоколом для передачі даних в Інтернеті. Використовується для взаємодії між клієнтами та серверами, а також може бути використаний в мережах Інтернету речей для отримання та відправлення даних.

DDS (Data Distribution Service) стандарт комунікації для розподіленого обчислення, включаючи системи Інтернету речей. DDS надає механізми для обміну даними між пристроями в реальному часі та управління якістю обслуговування.

WebSockets протокол, який дозволяє забезпечити двосторонній зв'язок між клієнтом та сервером через одне TCP-з'єднання. WebSockets часто використовуються для реального часу взаємодії між веб-додатками та пристроями IoT.

AMT (Application Management Protocol) використовується для управління та моніторингу пристроїв IoT. Забезпечує можливість віддаленого керування та надсилання команд пристроям.

XMPP (Extensible Messaging and Presence Protocol) протокол миттєвого обміну повідомлення, але його також можна використовувати для взаємодії пристроїв IoT, забезпечуючи широкі можливості комунікації.

Одна з оновлених версій протоколу HTTP, яка покращує швидкість передачі даних і може бути використана для ефективної комунікації між пристроями та серверами IoT.

Логічне проєктування є абстрактним розумінням ключових сутностей та процесів в системі Інтернету речей (IoT) та включає такі складові:

- функціональні блоки IoT є відокремленими елементами, які відповідають за різні аспекти системи IoT, такі як пристрої, зв'язок, послуги, управління та додатки;
- модель «зв'язку IoT» визначає структуру та засоби взаємодії між різними функціональними блоками в системі IoT;
- API зв'язку IoT інтерфейси програмування додатків, які визначають правила та можливості взаємодії між компонентами системи IoT.

Функціональні блоки IoT розподілені за таким чином:

- блок пристроїв відповідає за здатність пристроїв до зондування, моніторингу та управління;
- блок зв'язку обробляє всі аспекти зв'язку в системі IoT;
- блок управління забезпечує різні функції управління в системі Інтернету речей;
- блок безпеки відповідає за забезпечення безпеки системи IoT;
- блок додатків контролює різні аспекти в IoT, що стосуються застосувань.

Дане логічне проєктування дозволяє абстрагувати ключові концепції та функціональні елементи Інтернету речей, розглядаючи їх у взаємодії та об'єднуючи їх для досягнення мети системи IoT.

У сфері Інтернету речей використовуються різні моделі взаємодії, включаючи:

- модель «Запит-Відповідь» орієнтована на взаємодію між клієнтом і сервером, де клієнт відправляє запит, а сервер відповідає на цей запит.
- модель «Push-Pull» включає взаємодію система взаємодіє з пристроями, надсилаючи їм активні повідомлення (push) або очікуючи на їхні відповіді (pull).
- модель «Пар» передбачає взаємодію між пристроями у парі, де один пристрій може ініціювати дії, а інший може реагувати або відповідати.

API (інтерфейс програмування додатків) в Інтернеті речей часто використовують два основні підходи:

- API на основі REST використовує архітектурний стиль REST (представлення стану переносу), де ресурси доступні через стандартні HTTP-методи, такі як GET, POST, PUT і DELETE.
- API на основі WebSocket використовує технологію WebSocket для забезпечення двостороннього зв'язку між клієнтом і сервером в реальному часі [5].

Обидва API забезпечують зручний та ефективний засіб взаємодії між пристроями в Інтернеті речей, надаючи можливість обміну даними та керування пристроями через стандартні та передові інтерфейси.

Система Інтернету речей (IoT) складається з різноманітних пристроїв, які включають:

- три розумних дверних замка;
- три датчики відкриття вікна;
- дві розумні лампи;
- три датчики включення світла;
- одна базова станція, яка виступає в ролі шлюзу.

Щодо протоколів взаємодії, система використовує такі специфікації на різних рівнях:

- канальний рівень Wi-Fi технологія використовується для всіх сенсорів.
- мережевий рівень IPv4 протокол застосовується для мережевого з'єднання.
- транспортний рівень підтримуються TCP та UDP протоколи для передачі даних між пристроями та базовою станцією.
- рівень додатків використовуються протоколи MQTT та WebSocket для ефективної комунікації між пристроями.

Топологія IoT системи, представлена на рисунку 3.2 за допомогою PacketTracer, показує, що всі сенсори в системі підключені до мережі через шлюз. Даний шлюз відповідає за маршрутизацію даних та їх передачу. Мережа Інтернету речей ізольована та використовує адресацію 192.168.25.0/24. В системі реалізована

модель запит-відповідь і використовуються API зв'язку на основі REST і WebSocket для ефективного обміну даними та керування пристроями [6].

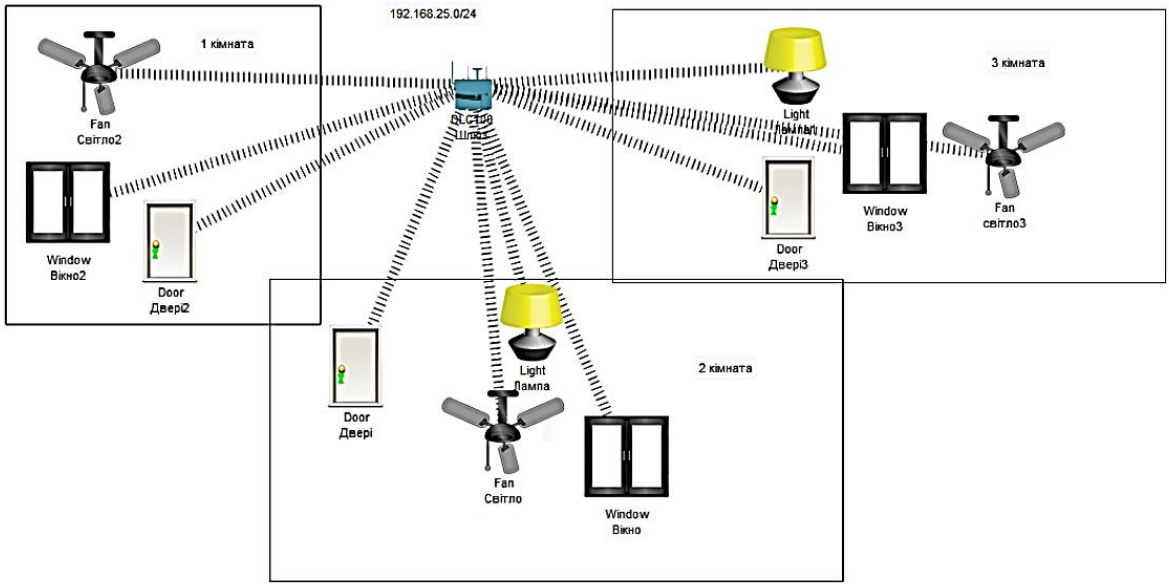
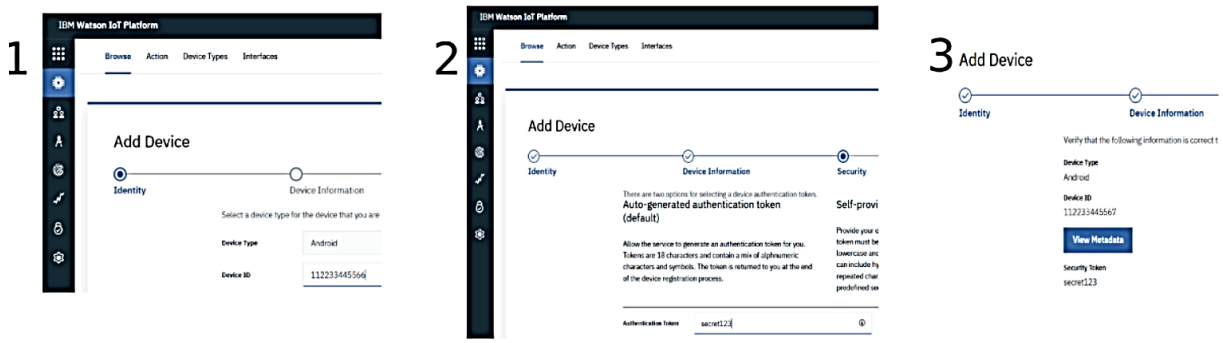


Рис.3.2. Архітектура Інтернету Речей

3.2. Визначення та впровадження засобів захисту в IoT мережах

В рамках забезпечення безпеки системи Інтернету речей (IoT) використовується метод TLS/SSL аутентифікації поверх протоколу MQTT.

У системі, де використовується протокол MQTT, вирішили застосувати метод автентифікації, додавши до нього шар TLS/SSL захисту. На рівні додатків, де використовується MQTT, інтегруємо SSL/TLS захист, що реалізований на платформі IBM Watson IoT Platform (рис.3.3, рис.3.4).



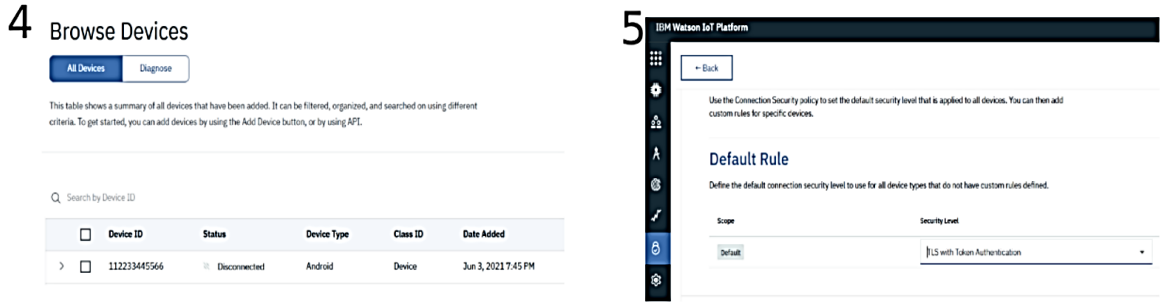


Рис.3.3. Створення пристрою в платформі Інтернету речей (IoT)

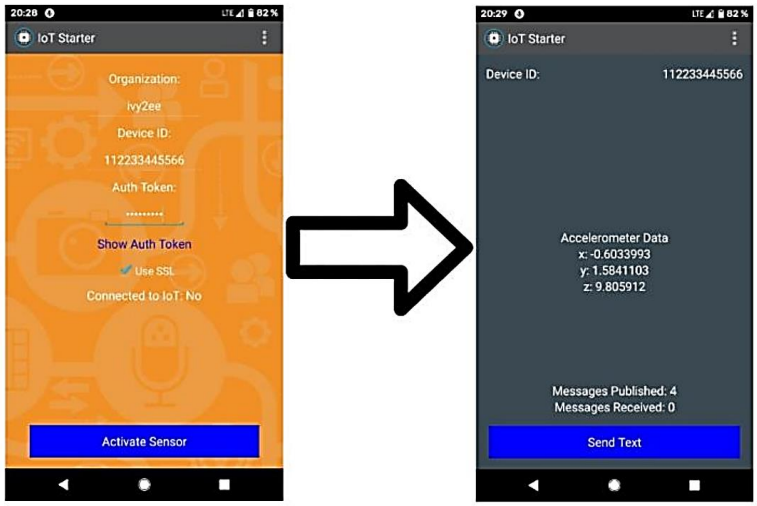


Рис.3.4. Підтвердження ідентифікації пристрою

Впровадження системи контролю доступу для пристроїв (рис. 3.5).

Створюємо нову роль та призначаємо конкретні права, редагуючи права для шлюзу та користувача.

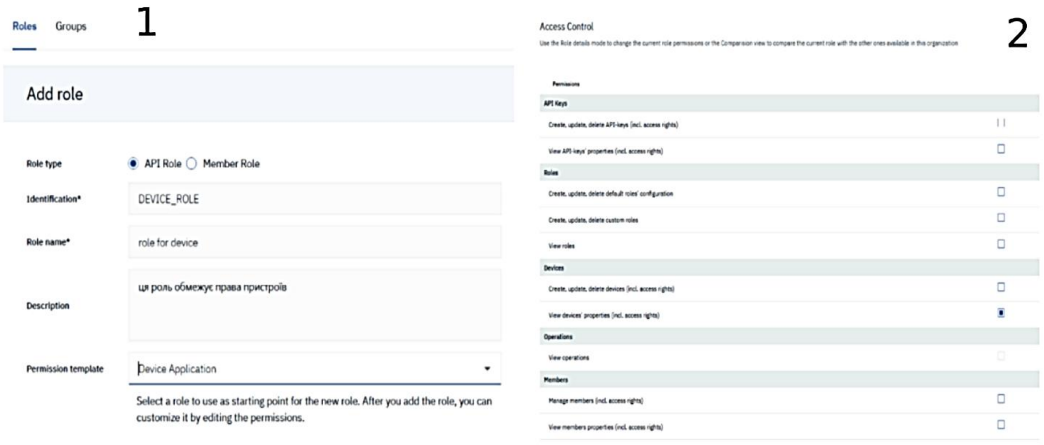


Рис.3.5. Впровадження апаратного методу забезпечення безпеки.

Для підвищення рівня безпеки під час обміну інформацією між пристроями Інтернету речей, був впроваджений модуль створення ключів шифрування.

Оптимальним рішенням є використання TPM-модуля, оскільки він володіє рядом важливих функцій (рис. 3.6):

– забезпечує цілісність пристрою;
– може функціонувати у безпечному режимі для мінімізації можливих шкідливих впливів при зараженні шкідливим програмним забезпеченням;

Встановлює корінь довіри.

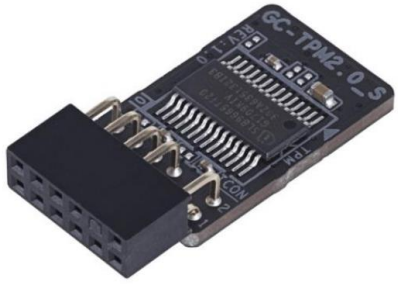


Рис.3.6. Модуль Trusted Platform Module (TPM).

Програмне забезпечення системи IoT створено для з'єднання сенсорів з хмаровою інфраструктурою. IoT-платформи розташовані між рівнем сенсорів та додатками. Замість того, щоб датчик ініціював підключення до хмари, цю роль відіграє смартфон. Після створення пристрою завантажити додаток на смартфон і проходити етап аутентифікації для безпечного підключення до платформи.

Використання TLS/SSL аутентифікації поверх MQTT віддзеркалює підхід до забезпечення конфіденційності та безпеки обміну даними в системі Інтернету речей. При такому підході кожне підключення аутентифікується та захищається за допомогою шифрування, що важливо для забезпечення конфіденційності та недопущення несанкціонованого доступу до передаваної інформації.

Забезпечення зв'язку в IoT:

Реалізація шифрування та перевірки аутентичності. Дослідження виявило, що більшість систем Інтернету речей (IoT) практично не застосовують шифрування для трафіку, що створює серйозні загрози безпеці. У відповідь на це, виникає

необхідність у впровадженні ключових аспектів для забезпечення безпеки зв'язку в системах IoT.

Шифрування трафіку. В проєктуванні мережі використовується метод Еліптичної криптографії для шифрування трафіку. Метод відзначається високою швидкістю, особливо на обмежених за ресурсами чіпах, що є важливим для ефективної роботи в умовах IoT.

Перевірка аутентичності. В систему впроваджено сертифікат безпеки X.509 для надання унікальної ідентифікації пристрою. Дозволяє визначити, які пристрої є довіреними, підвищуючи рівень безпеки в мережі. Перевірка аутентичності грає важливу роль у виключенні неперевірених пристроїв і сервісів з мережі, що є критично важливим для запобігання атакам [7].

Безпека пристроїв на рівні коду в IoT

Захищеність коду від несанкціонованого використання. З метою уникнення включення пристроїв до ботнетів та запобігання їх участі в шкідливих діях, необхідно забезпечити, щоб пристрої виконували лише покладені на них функції. Одним із ключових заходів в цьому контексті є створення захищеного коду для пристроїв Інтернету речей (IoT).

Реалізація запропонованих рішень в IoT системі. Вибір OpenSSL для перевірки аутентичності та підтвердження виконавчого коду. При проєктуванні системи визначено використання бібліотеки OpenSSL для здійснення перевірки автентичності та підтвердження необхідного виконавчого коду на пристрої. Це важливий етап, оскільки забезпечує можливість перевірки та автентифікації коду, що виконується на пристрої, та забезпечує виключення несанкціонованого використання або модифікації коду.

Забезпечення безпеки коду на рівні програмного забезпечення пристроїв є критично важливим кроком для забезпечення їх надійності та виключення можливості їх використання для шкідливих цілей. Використання бібліотеки OpenSSL є стратегічним вибором для гарантії відповідності коду пристроїв встановленим стандартам безпеки.

У контексті безпеки при використанні пристроїв IoT, виявлені загрози, такі як шкідливе програмне забезпечення, компрометація пристрою та вразливості, вимагають систематичного підходу для їх уникнення та мінімізації ризиків.

Впровадження системи розмежувань доступу, яка повністю обмежує взаємодію між мережевими підключеннями та додатками, що значно підвищило рівень захисту від потенційних експлойтів та компрометації.

Використання системи аналітики інформаційної безпеки (UBA), яка виявляє аномальну поведінку користувача. Система акумулює різноманітну інформацію, будує модель поведінки та виявляє аномалії в активності [8].

Додаткові практики для поліпшення безпеки:

Регулярні оновлення IoT пристроїв для вчасної установки патчів та виправлення вразливостей.

- встановлення та використання антивірусного програмного забезпечення Symantec для захисту від різних видів вірусів.
- місячні аудити інфраструктури мережі за допомогою сервісу AWS IoT Device Defender для забезпечення безпеки.
- використання брандмауера для контролю вхідного та вихідного трафіку на пристроях IoT.
- генерація та періодична зміна надійних та унікальних паролів.
- використання ізольованої мережі з підмережею 192.168.25.0/24 для ускладнення несанкціонованого доступу.

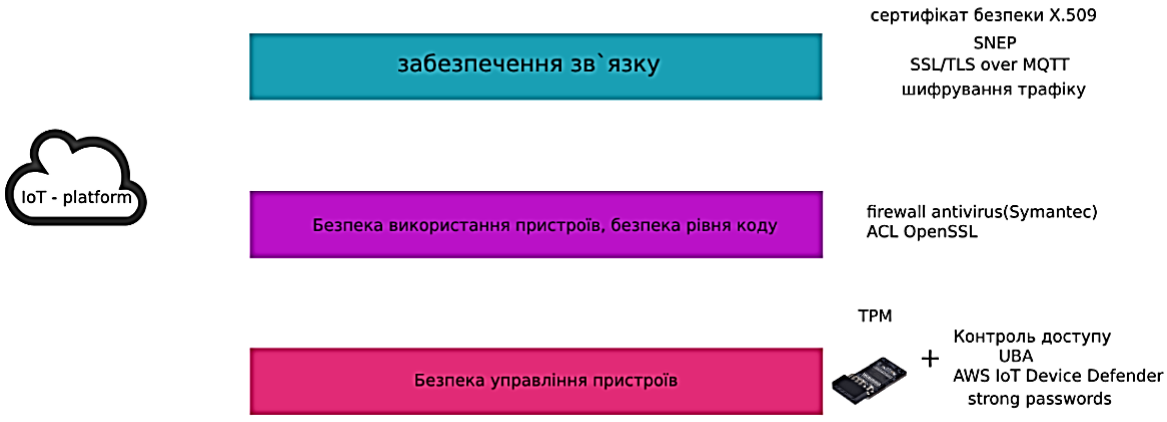


Рис. 3.7 Забезпечення безпеки в системі IoT: використані методи

Графічне зображення використаних методів безпеки для спроєктованої системи IoT представлено на рисунку 3.7. Дані заходи спрямовані на створення найвищого рівня безпеки та впевненості в функціонуванні пристроїв IoT у вимогливих середовищах.

Поміж системи ідентифікації та управління доступом (IAM), реалізація привілейованої системи управління користувачами відстежує активність та взаємодію адміністраторів, адміністративних консолей та додатків. Це особливо корисно у великих мережевих системах Інтернету речей (IoT) та допомагає визначати політику облікових записів, автоматично оновлювати паролі після кожного використання, видаляти та надавати облікові записи, а також реєструвати активність, наприклад, натискання клавіш для цілей криміналістики.

Щодо ідентифікації споживачів, особливо в галузі роздрібної торгівлі чи транспорті, існують концепції централізованих систем, що ґрунтуються на політиці та базуються на згоді, дозволяючи споживачам контролювати:

- які їхні атрибути чи інформація можуть бути чіткими;
- яку інформацію слід маскувати під час відображення;
- яку інформацію можуть використовувати сторонні аналітики та маркетинг;
- інші уподобання.

На основі всього вищезазначеного можна побудувати блок-схему для створення безпечної мережі Інтернету речей (IoT), яка представлена на рисунку 3.8. За допомогою описаних у цій схемі кроків та інших вказівок у даній роботі, фахівці можуть розробити та впровадити IoT мережу будь-якого масштабу для будь-якого підприємства. Дана схема проілюстрована на рисунку 3.8.

Рис.3.8. Система побудови безпечної IoT мережі.

3.3. Аутентифікація та Авторизація

Гарантування ефективної аутентифікації та авторизації пристроїв у мережі Інтернету речей (IoT) є ключовим для забезпечення безпеки та контролю за доступом окремих користувачів і пристроїв. У цьому контексті програмне забезпечення повинно впроваджувати механізми, спрямовані на забезпечення безпечності в цьому електронному середовищі. На приклад, можна використовувати такі механізми, як двофакторна аутентифікація та ролева модель доступу.

Аутентифікація – це процес перевірки особи користувача, пристрою або служби, який дає змогу отримати авторизований доступ до конфіденційної інформації або

систем. Авторизація, з іншого боку, – це процес надання або відмови в доступі до ресурсу на основі дозволів аутентифікованого користувача.

Аутентифікація та авторизація є важливими поняттями в комп'ютерній безпеці, особливо в контексті мережі Інтернету речей (IoT), де пристрої та користувачі повинні мати можливість безпечно взаємодіяти один з одним. Програмне забезпечення повинно підтримувати механізми, такі як двофакторна аутентифікація та ролева модель доступу, щоб забезпечити правильну аутентифікацію та авторизацію пристроїв у мережі IoT.

Двофакторна аутентифікація (2FA) – це метод, який вимагає від користувачів двох форм автентифікації для доступу до системи або додатка. Наприклад, користувач може ввести пароль та отримати одноразовий код на свій мобільний пристрій. Це збільшує рівень безпеки, оскільки потенційний зловмисник повинен мати доступ до обох факторів, щоб отримати доступ до системи.

Ролева модель доступу (RBAC) – це метод, який визначає дозволи на основі ролей користувачів, а не на основі індивідуальних особистостей. Наприклад, користувач, який має роль адміністратора, може мати повний доступ до всіх функцій та даних системи, тоді як користувач, який має роль оператора, може мати обмежений доступ до певних функцій та даних. Це спрощує управління доступом та зменшує ризик несанкціонованого доступу.

Платформа управління Інтернетом речей (IoT Management Platform) – це програмне забезпечення, яке дозволяє підключати, керувати та аналізувати дані з різних пристроїв, які використовують технологію Інтернету речей (IoT). За допомогою платформи IoT ви можете створювати розумні та інноваційні рішення для вашого бізнесу, які покращують продуктивність, ефективність, безпеку та зручність.

Платформа IoT складається з трьох основних компонентів:

Обладнання – це фізичні пристрої, які підключені до мережі Інтернету та збирають та передають дані. Це можуть бути сенсори, датчики, виконавчі механізми, камери, роботи тощо.

Підключення – це канали, через які пристрої обмінюються даними між собою або з хмарним сховищем. Це можуть бути різні протоколи та технології, такі як Wi-Fi, Bluetooth, LoRaWAN, NB-IoT, 5G тощо.

Програмне забезпечення – це аналітичний модуль, який отримує дані від пристроїв, обробляє та аналізує їх, видає команди на виконавчі механізми, залежно від налаштувань, встановлених користувачем. Це також включає інтерфейс користувача, який дозволяє візуалізувати та контролювати дані та пристрої.

Платформа IoT може мати різні функції та можливості, залежно від сфери застосування та потреб користувачів. Деякі з них можуть бути:

- Масштабованість – здатність підключати та керувати великою кількістю пристроїв, які можуть змінюватися в часі.
- Багатофункціональність – здатність відпрацьовувати сценарії автоматизованого керування різними типами пристроїв для різного бізнесу.
- Безпека – здатність захищати дані та пристрої від несанкціонованого доступу, злому, втрати або пошкодження.
- Інтеграція – здатність співпрацювати з іншими системами, додатками, сервісами або платформами, що використовуються користувачами.

Програмне забезпечення для забезпечення аутентифікації та авторизації в мережі Інтернету Речей (IoT) має функціональні властивості:

Двофакторна аутентифікація (2FA): У користувачів платформи IoT може вимагатися введення свого користувацького пароля та додаткового одноразового коду, який вони отримають через мобільний додаток або електронну пошту. Це забезпечує додатковий рівень безпеки, оскільки навіть у випадку витоку пароля, зловмисники повинні мати доступ і до додаткового коду для успішного входу.

Ролева модель доступу: Визначення різних ролей, таких як адміністратор, користувач, та гость. Адміністратор може мати повний доступ до всіх пристроїв і функцій, користувач обмежений в деяких можливостях, а гість може тільки переглядати обмежену кількість даних. Це забезпечує контроль за тим, хто та як використовує функціонал платформи, і уникнення несанкціонованого доступу.

У *третьому розділі «Програмне забезпечення безпечної системи Інтернету речей (IoT)»* ретельно розглянули завдання, виклики та різні аспекти проєктування безпечної системи Інтернету речей (IoT). Визначили основні завдання для проєктування IoT системи, зокрема, зосереджуючись на фізичному та логічному проєктуванні мережі, а також врахуванні архітектурних рівнів.

Висвітлено визначення та впровадження засобів захисту в IoT мережах, розглянуті протоколи на різних рівнях мережі, включаючи канальний, мережевий, транспортний та рівень додатків. Розглядалися аспекти аутентифікації, авторизації та інші методи забезпечення безпеки.

Особливий акцент був зроблений на важливості аутентифікації та авторизації в IoT системах, оскільки ці процеси визначають, які пристрої мають доступ до системи та яким чином цей доступ контролюється.

Наведені приклади використання апаратних засобів безпеки, зокрема TPM-модулів, підкреслили важливість фізичного захисту пристроїв та ключових елементів інфраструктури.

Результатом розділу є глибоке розуміння проблем та можливих рішень у сфері програмного забезпечення для систем Інтернету речей, яке буде використано при подальшому розробленні та вдосконаленні безпечних IoT систем.

ВИСНОВОКИ

Кожна система Інтернету речей (IoT) потребує унікального та комплексного підходу до забезпечення інформаційної безпеки, оскільки на сьогоднішній день немає універсальних умов і вимог для цього.

Безпеку IoT слід розглядати з різних точок зору при проєктуванні, оскільки в іншому випадку вона може виявитися неефективною, і зловмисники можуть використовувати слабкі сторони системи. У даній статті було акцентовано увагу на таких компонентах:

- створення і проєктування системи IoT визначено основні компоненти IoT і виконано аналіз загроз безпеки та вразливостей на різних рівнях системи;
- методи забезпечення інформаційної безпеки в IoT.

Запропоновано різні методи безпеки для різних аспектів системи IoT, таких як забезпечення зв'язку, безпека пристроїв на рівні коду, безпека використання пристроїв та управління безпекою пристроїв.

Дане дослідження включає в себе вивчення ключових аспектів безпеки в Інтернеті речей та розробку конкретних методів та стратегій для захисту інформації в мережі IoT від несанкціонованого доступу. Запропоновані методи та рекомендації можуть служити основою для розробки ефективних систем безпеки в майбутніх проєктах IoT.

Використання TLS/SSL аутентифікації поверх MQTT в системі IoT є одним із прикладів ефективного застосування сучасних методів безпеки. Висунуті рекомендації та розроблені стратегії можуть служити основою для практичної реалізації безпеки в конкретних проєктах Інтернету речей, а також допомагати у подальшому розвитку методологій захисту в цьому напрямку.

У висновку дослідження важливо визначити, що безпека в Інтернеті речей (IoT) вимагає індивідуального та комплексного підходу, оскільки кожна система має свої унікальні вимоги та умови. Враховуючи динаміку та постійні зміни в цьому секторі, підходи до захисту систем IoT повинні бути гнучкими та адаптованими.

ПЕРЕЛІК ПОСИЛАНЬ

1. “ H. Wang, J. Zhang: Blockchain Based Data Integrity Verification” – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8895808
2. “7 design principles for IoT” – Режим до ресурсу:https://futurice.com/blog/7-design-principles-for-iot
3. “Internet of Things: security and privacy implications” – Режим доступу до ресурсу:https://www.researchgate.net/publication/275228804_Internet_of_Thingsecurity_and_privacy_implications
4. “IoT Architecture: the Pathway from Physical Signals to Business Decisions” – Режим доступу до ресурсу: https://www.altexsoft.com/blog/iotarchitecture-layers-components/
5. “IoT Privacy and Security: Challenges and Solutions” ” – Режим доступу до ресурсу: https://www.mdpi.com/2076-3417/10/12/4102/pdf
6. “Privacy” – Режим доступу до ресурсу: https://www.gsma.com/aboutus/legal/privacy
7. “RFID and Inclusive Model for the Internet of Things” – Режим доступу до ресурсу:https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf
8. “Особенности защиты информации в Интернете вещей” – International Journal of Open Information Technologies ISSN: 2307-8162 vol. 6, no.10, 2018
9. A Review of Blockchain in Internet of Things and AI Big Data Cogn. Comput., 2020 Licensee MDPI, Basel, Switzerland
10. Analysis of the Cryptographic Tools for Bockchain and Bitcoin – Режим доступу до ресурсу: https://www.mdpi.com/2227-7390/8/1/131/htm
11. Assisting Users ina World Full of Cameras: A Privacy-Aware Infrastructure for Computer Vision Applications. In CVPRW. IEEE, 1387–1396.

12. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, “Blockchain based data integrity service framework for IoT data, in Proc. ICWS”, Jun. 2017.” – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8029796
13. Barry Haughian Design, Launch, and Sacle IoT Services: A Practical Business Approach / Barry Haughian: Apress, 2018. – 292 p.
14. Brian Russel Practical Internet of Things Security / Brian Russel, Drew Van Duren: Packt Publishing, 2018. – 382 p.
15. C. Wang, S. Chen, Z. Feng, Y. Jiang, and X. Xue, “Block chain-based data audit and access control mechanism in service collaboration, in Proc. ICWS”, Jul – Режим доступу до ресурсу: https://ieeexplore.ieee.org/abstract/document/8818439
16. Claire Rowland User Experience Design for the Internet of Things / Claire Rowland: O'Reilly Media, Inc., 2015.
17. Cyber risk in an Internet of Things world: deloitte. Available at: https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-aninternet-of-things-world-emerging-trends.html
18. Cybersecurity and the Internet of Things: security. Available at: https://www.securitymagazine.com/articles/90793-cybersecurity-and-the-internet-of-things
19. D. Wyatt, T. Choudhury, and J. Bilmes. 2007. Conversation detection and speaker segmentation in privacy-sensitive situated speech data. InInterspeech.
20. D. Yue, R. Li, Y. Zhang, W. Tian, and C. Peng, “Blockchain based data integrity verification in P2P cloud storage,in Proc. ICPADS”, Dec. 2018 – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8644863
21. Dac-Nhuong Le IoT: Security and Privacy Paradigm / Dac-Nhuong Le, Souvik Pal: CRC Press, 2020. – 399 p.
22. Demystifying Internet of Things Security: Design a security framework for an Internet connected ecosystem / Sunil Cheruvu, Anil Kumar, Ned Smith, David M. Wheeler : Apress, 2019. – 382 p.

23. Fei Hu Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations / Fei Hu: CRC Press, 2016. – 604 p.
24. Gilad Rosner Privacy and the Internet of Things / Galid Rosnar: O'Reilly Media, Inc., 2016.
25. Good Practices for Security of Internet of Things in the context of Smart Manufacturing: enisa. Available at: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot?fbclid=IwAR1qchv88kZRsIESHtGTEwbA0Mbx8mb9hV1Euqy-Y--IHVYvLuFhGuvi6o
26. Informacionnaya bezopasnost' interneta veshchej (Internet of Things) [Information security of the internet of things]: TADVISER. Available at: https://goo.su/2l3u
27. Internet of Things (IoT) security: 9 ways you can help protect yourself: Norton. Available at: https://us.norton.com/internetsecurity-iot-securing-the-internet-of-things.html
28. Internet of Things (IOT) security: imperva. Available at: https://www.imperva.com/learn/applicationsecurity/iot-internet-of-things-security/
29. Internet of Things: Asurvey on the security of IoT frame works/ Mahmoud Ammara, Giovanni Russellob,Bruno Crispo 2017p.
30. IoT Security / Madhusanka Liyanage, An Braeken, Pardeep Kumar, Mika Ylianttila: Wiley, 2020. – 304 p.
31. Ivanchuk O.V., Zavgorodii V.V., Kozel V.M., Drozdova Ye.A. Analiz protokoliv obminu danymy dlia keruvannia systemamy internetu rechei [Analysis of data exchange protocols for managing Internet of Things systems]. Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Tekhnichni nauky - Scientific notes of TNU named after VI Vernadsky. Series: Technical Sciences, 2020, no.2(31). pp. 99-104. doi: 10.32838/2663-5941/2020.2-1/15
32. JA Stankovic. 2014. Research directions for the internet of things. IEEE Internet of Things Journal 1, 1 (2014), 3–9.

33. Jaimunk, J. (2019). Privacy-Preserving Cloud-IoT Architecture (Abstract). 2019 IEEE/ACM 6th International Conference on Mobile Software Engineering and Systems (MOBILESoft).
34. K. Alanezi and S. Mishra, “A privacy negotiation mechanism for the internet of things,” in IEEE 16th International Conference on Dependable, Autonomic and Secure Computing, 16th International Conference on Pervasive Intelligence and Computing, 4th International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2018, pp. 512–519.
35. L. Cranor. 2002. Web privacy with P3P. " O’Reilly Media, Inc." A. Das, M. Degeling, X. Wang, J. Wang, N. Sadeh, and M. Satyanarayanan. 2017.
36. M. BinJubier et al.: Comprehensive Survey on Big Data Privacy Protection –Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8943156
37. M. Mun, S. Hao, N. Mishra, K. Shilton, J. Burke, D. Estrin, M. Hansen, and R. Govindan, “Personal Data Vaults:A Locus of Control for Personal Data Streams,” in Proceedings of the 6th International COnference, ser. Co-NEXT’10. New York, NY, USA: ACM, 2010, pp. 17:1–17:12.
38. P. Yang et al.: Data Security and Privacy Protection for Cloud Storage: A Survey – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9142202
39. PE Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. Cranor, and N. Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In SOUPS.
40. Practical IoT Hacking / Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods : No Starch Press, 2021. – 434 p.
41. Problemy i zadachi realizacii koncepcii Interneta Veshchej [Problems and tasks of implementing the concept of the Internet of Things]: habr. Available at: https://habr.com/ru/post/479890/
42. Rakjumar Buyya Internet of Things / Rajkumar Buyya, Amir Vahid Dastjerdi: Morgan Kaufmann, 2016. – 378 p.

43. S. Aljanabi, A. Chalechale: Improving IoT Services Using an HFCO – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328240
44. Security in the Internet of Things: mckinsey. Available at: https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things#.
45. Sravani Bhattacharjee / Practical Industrial Internet of Things Security: A Practitioner's Guide to Securing Connected Industries / Sravani Bhattacharjee: Packt Publishing, 2018. – 324 p.
46. The Web of Things: interconnecting devices with high usability and performance/ Simon Duquennoy, Jean-Jacques Vandewalle. 2019p.
47. Top 10 Biggest IoT Security Issues: intellectsoft. Available at: https://www.intellectsoft.net/blog/biggest-iot-security-issues/
48. Towards Secured Online Monitoring for Digitalized GIS Against CyberAttacks Based on IoT and Machine Learning – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9440436
49. U. Khadam et al.: Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8713871
50. V. Hassija et al.: Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures – Режим доступу до ресурсу: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8742551
51. What is AWS [Електронний ресурс]–Режим доступу до ресурсу: https://aws.amazon.com/what-is-aws/.
52. What is IoT Security (Internet of Things)? - Tools & Technologies: hackr. Available at: https://hackr.io/blog/what-is-iot-security-technologies.
53. What is IoT? The internet of things explained: NETWORKWORLD. Available at: https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html

54. What is the IoT? Everything you need to know about the Internet of Things right now: zdnet. Available Available at: https://www.zdnet.com/article/how-5g-can-help-unlock-iots-potential//
55. XIII Міжнародна науково-технічна конференція студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем" (ПРІТС-2020) «ІНФОРМАЦІЙНА БЕЗПЕКА INTERNET OF THINGS» Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2020/paper/view/20784/10840
56. XIII Міжнародна науково-технічна конференція студентів та аспірантів "Перспективи розвитку інформаційно-телекомунікаційних технологій та систем" (ПРІТС-2021) «ПРОБЛЕМИ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS» Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2021/paper/view/23215/12586
57. Богуш В. М., Кривуца В. Г., Кудін А. М., «Інформаційна безпека: Термінологічний навчальний довідник» За ред. Кривуці В. Г. Київ. 2004. 508 с.
58. Богуш В. М., Юдін О. К. «Інформаційна безпека держави». К.: «МКПрес», 2005. 432с.
59. Вєртузаев М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник/За ред. С.Г. Лаптєва. К.: Видавництво Європейського університету, 2001. 201 с.
60. Захист інформаційних ресурсів: навчально-методичний посібник до курсу “Захист інформаційних ресурсів” укл. С. О. Троян. Умань: 2012. 120 с.
61. Internet of things (IoT): IoTAgenda. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT /
62. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. Х.: НХУ України, 2004.
63. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: Кондор, 2004. 384 с.
64. Лаптєв О.А. Методологічні основи автоматизованого пошуку цифрових засобів негласного отримання інформації. К. Міленіум. 2020. 326 с.

65.Лєнков С. В., Перегудов Д. А., Хорошко В. А. Методи та засоби захисту інформації (в 2-ох томах). К: Арий, 2008.

66.НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, введений в дію Наказом ДСТСЗІ від 28.04.1999 р. № 22

67.Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. Х.: НХУ України, 2004.

68.Пороло Є. Застосування концепції Data Bank в мережі хмарного IoT / Євгеній Пороло // ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТА СИСТЕМ / Євгеній Пороло. – м. Київ, Україна: ISSN (print)2663-502X, ISSN (online) 2664-3057, 2020. –С. 368.

69.Пороло Є. Удосконалена архітектура мережі для хмарного Інтернету речей / Є. Пороло, В. Курдеча // ПЕРСПЕКТИВИ ТЕЛЕКОМУНІКАЦІЙ / Є. Пороло, В. Курдеча. – м. Київ, Україна: ISSN(print) 2663-502X, ISSN(online) 2664-3057, 2020. – С. 219 – 221.

70.Росоловський В.М., Анкудович Г.Г., Катерноза К.О., Шевченко М.Ю. Основи інформаційної безпеки автоматизованої інформаційної системи державної податкової служби України: Навч. Посібник /За ред. М.Я. Азарова. Ірпінь: Академія ДПС України, 2003. 466 с.

71. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник. К.: КНТ, 2007.

72.Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: Навчальний посібник / В.С. Сідак, В.Ю. Артемов. К.: Вид-во КНТ, 2007.

73. XV Міжнародна науково-технічна конференція "Перспективи телекомунікацій 2021" (ПТ-2021) «АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В МЕРЕЖІ INTERNET OF THINGS» Режим доступу до ресурсу: http://conferenc.its.kpi.ua/2021/paper/view/23277/12581

74.Харченко В.С. Інформаційна безпека: глосарій / В.С. Харченко. К.: Видво КНТ, 2005. 13-18 с.

Презентаційні матеріали

Регулярні оновлення IoT пристроїв для вчасноїустановки патчів та виправлення вразливостей.

Забезпечення безпеки в системі IoT: використані методи

- встановлення та використання антивірусного програмного забезпечення Symantec для захисту від різних видів вірусів.
- місячні аудити інфраструктури мережі за допомогою сервісу AWS IoT Device Defender для забезпечення безпеки.
- використання брандмауера для контролю вхідного та вихідного трафіку на пристроях IoT.
- генерація та періодична зміна надійних та унікальних паролів.
- використання ізольованої мережі з підмережею 192.168.25.0/24 для ускладнення несанкціонованого доступу.

Забезпечення зв'язку в IoT:

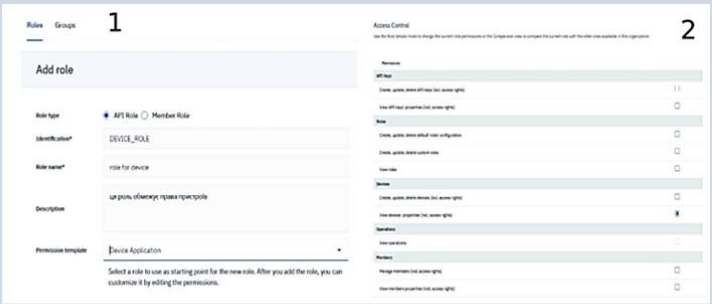
Реалізація шифрування та перевірки аутентичності. Дослідження виявило, що більшість систем Інтернету речей (IoT) практично не застосовують шифрування для трафіку, що створює серйозні загрози безпеці. У відповідь на це, виникає необхідність у впровадженні ключових аспектів для забезпечення безпеки зв'язку в системах IoT.

Шифрування трафіку. В проєктуванні мережі використовується метод Еліптичної криптографії для шифрування трафіку. Метод відзначається високою швидкістю, особливо на обмежених за ресурсами чіпах, що є важливим для ефективної роботи в умовах IoT.

Перевірка аутентичності. В систему впроваджено сертифікат безпеки X.509 для надання унікальної ідентифікації пристрою. Дозволяє визначити, які пристрої є довіреними, підвищуючи рівень безпеки в мережі. Перевірка аутентичності грає важливу роль у виключенні неперевірених пристроїв і сервісів з мережі, що є критично важливим для запобігання атакам.

Впровадження системи контролю доступу для пристроїв. Створюємо нову роль та призначаємо конкретні права, редагуючи права для шлюзу та користувача.

Для підвищення рівня безпеки під час обміну інформацією між пристроями Інтернету речей, був впроваджений модуль створення ключів шифрування.

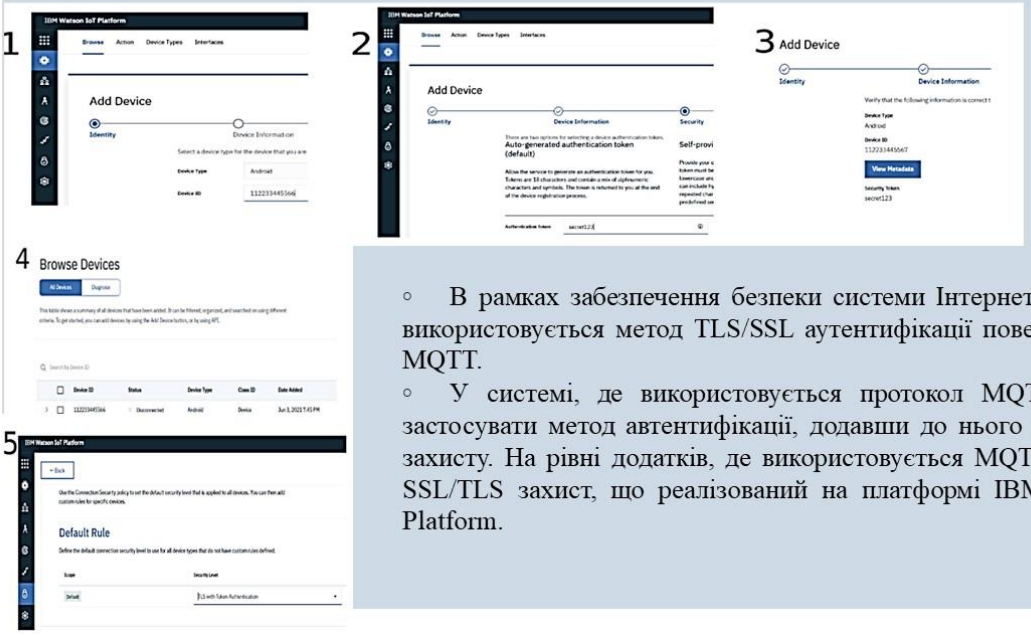


Оптимальним рішенням є використання TPM-модуля, оскільки він володіє рядом важливих функцій:

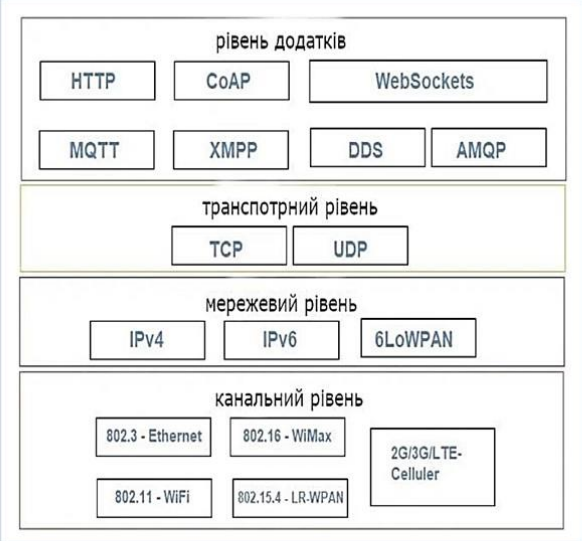
- забезпечує цілісність пристрою;
- може функціонувати у безпечному режимі для мінімізації можливих шкідливих впливів при зараженні шкідливим програмним забезпеченням.

Встановлює корінь довіри.

Визначення та впровадження засобів захисту в IoT мережах



- В рамках забезпечення безпеки системи Інтернету речей (IoT) використовується метод TLS/SSL аутентифікації поверх протоколу MQTT.
- У системі, де використовується протокол MQTT, вирішили застосувати метод автентифікації, додавши до нього шар TLS/SSL захисту. На рівні додатків, де використовується MQTT, інтегруємо SSL/TLS захист, що реалізований на платформі IBM Watson IoT Platform.



Протоколи для зв'язку в Інтернеті Речей

Фізичне планування мережі включає в себе розгляд пристроїв IoT та використання протоколів. Існує ряд протоколів на різних рівнях, які забезпечують ефективне управління та взаємодію між пристроями IoT та серверами через Інтернет.

Протоколи *канального рівня* в мережі Інтернету речей (IoT) відіграють важливу роль у забезпеченні ефективного та безпечного обміну даними між пристроями.

Протоколи *мережевого рівня* визначають, як дані передаються між різними пристроями в мережі.

Протоколи *транспортного рівня* виконують ключові завдання у забезпеченні передачі даних між пристроями в мережі, забезпечуючи надійність і контроль цілісності.

Протоколи *рівня додатків* в мережах Інтернету речей (IoT) використовуються для взаємодії та обміну даними між різнорідними пристроями та системами.

Логічне проєктування є абстрактним розумінням ключових сутностей та процесів в системі Інтернету речей (IoT) та включає такі складові:

- функціональні блоки IoT є відокремленими елементами, які відповідають за різні аспекти системи IoT, такі як пристрої, зв'язок, послуги, управління та додатки;
- модель «зв'язку IoT» визначає структуру та засоби взаємодії між різними функціональними блоками в системі IoT;
- API зв'язку IoT інтерфейси програмування додатків, які визначають правила та можливості взаємодії між компонентами системи IoT.

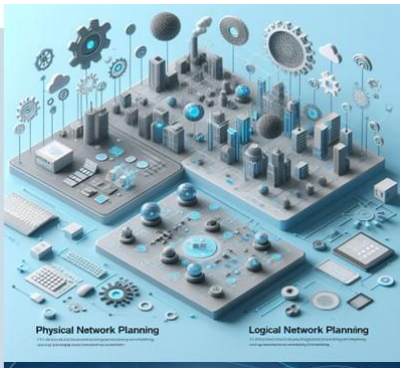
Функціональні блоки IoT розподілені за таким чином:

- блок пристроїв відповідає за здатність пристроїв до зондування, моніторингу та управління;
- блок зв'язку обробляє всі аспекти зв'язку в системі IoT;
- блок управління забезпечує різні функції управління в системі Інтернету речей;
- блок безпеки відповідає за забезпечення безпеки системи IoT;
- блок додатків контролює різні аспекти в IoT, що стосуються застосувань.

Визначення завдань для проєктування системи Інтернету речей (IoT)

При розробці мережі Інтернету речей необхідно враховувати два аспекти:

- фізичне планування мережі;
- логічне планування мережі.



У третьому розділі «Програмне забезпечення безпечної системи Інтернету речей (IoT)» ретельно розглянули завдання, виклики та різні аспекти проєктування безпечної системи Інтернету речей (IoT). Визначили основні завдання для проєктування IoT системи, зокрема, зосереджуючись на фізичному та логічному проєктуванні мережі, а також врахуванні архітектурних рівнів.

Висвітлено визначення та впровадження засобів захисту в IoT мережах, розглянуті протоколи на різних рівнях мережі, включаючи канальний, мережевий, транспортний та рівень додатків. Розглядалися аспекти аутентифікації, авторизації та інші методи забезпечення безпеки.

Особливий акцент був зроблений на важливості аутентифікації та авторизації в IoT системах, оскільки ці процеси визначають, які пристрої мають доступ до системи та яким чином цей доступ контролюється.

РОЗДІЛ 3.
ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Засоби та системи для виявлення, пошуку та нейтралізації технічних засобів, що вилучають інформацію

Мережевий захищений комплекс (МТК) розроблено для надійного обміну різними видами інформації, такими як дані, відео та аудіо, на високому рівні конфіденційності.

Комплектація МТК включає у себе мережеве обладнання, засоби криптографічного захисту інформації (шифратори), систему електроживлення та інші компонент.

При обміні захищеною інформацією між КП використовуються протоколи IPsec, які включають такі компоненти:

- ESP (Encapsulating Security Payload) – протокол для шифрування та аутентифікації даних.
- AH (Authentication Header) – протокол для аутентифікації джерела та цілісності даних.

Схема використання

Засоби та системи для виявлення, пошуку та нейтралізації технічних засобів, що вилучають інформацію

Засоби та системи для захисту Інтернету речей (IoT):

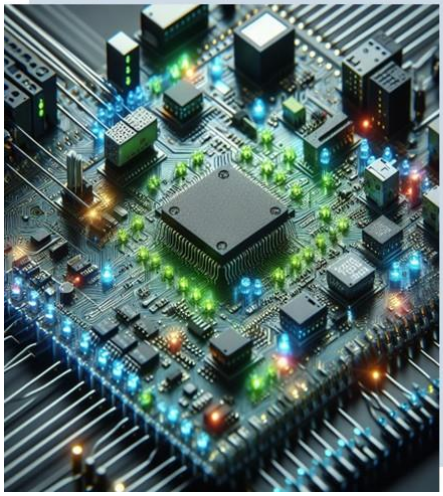
•**Виявлення:** Використовуються системи виявлення вторгнень (IDS) для ідентифікації аномальних патернів, що можуть вказувати на потенційні загрози.

•**Пошук:** Системи управління подіями в області безпеки інформації (SIEM) збирають та аналізують дані з різних джерел для виявлення потенційних загроз.

•**Нейтралізація:** Застосовуються різні технології, включаючи шифрування, аутентифікацію, мережеві брандмауери та системи запобігання вторгненням (IPS), для нейтралізації ідентифікованих загроз.

Схема використання

Основні аспекти розділу включають апаратний захист інформації, стаціонарні засоби захисту, системи для виявлення та нейтралізації технічних засобів, що вилучають інформацію, використання криптографічних засобів у системах захисту інформації та аспекти безпеки бездротових мереж передачі даних та на необхідність комплексного підходу до апаратного захисту Інтернету речей, оскільки відмічається постійний розвиток технологій та зростання загроз кібербезпеці.



Розглядаються різноманітні засоби та системи, які сприяють виявленню та нейтралізації потенційних загроз, а також підкреслюється важливість використання криптографічних методів для захисту інформації. Бездротові мережі передачі даних визначаються як ключовий елемент, вимагаючи особливої уваги до їхньої безпеки.

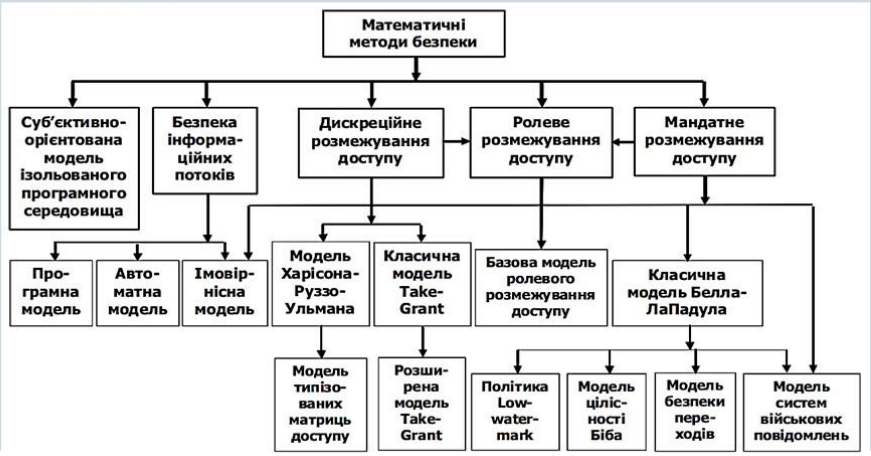
Другий розділ «Апаратне забезпечення безпечної системи інтернету речей (IoT)» присвячений апаратному забезпеченню системи Інтернету речей (IoT), де розглянуто різноманітні аспекти безпеки та захисту інформації. На основі досліджень пропонуються рішення та технічні засоби для забезпечення ефективного функціонування та захисту системи IoT.

РОЗДІЛ 2.

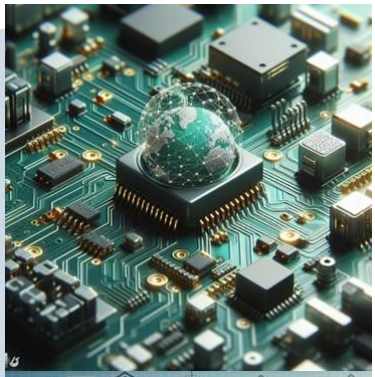
АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

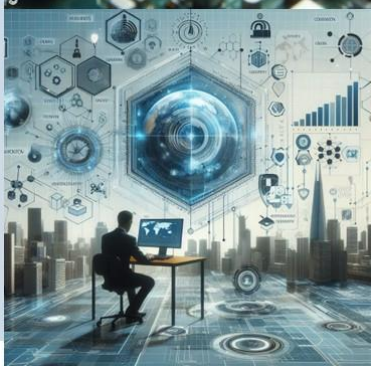
Математичні визначення безпеки систем

Математична модель безпеки – це формальне визначення політики безпеки. Згідно вимог нормативних документів у галузі захисту інформації в інформаційних системах, системи захисту інформації будуються на основі математичних моделей, які дозволяють теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки. Розвиток формальної теорії захисту інформації, хоч і недавній, вже призвів до створення численних математичних моделей, що описують різні аспекти безпеки та надають теоретичну базу для побудови сучасних систем захисту інформації



- *LPWAN* (малопотужна широкосмугова мережа) спеціально розроблена для пристроїв IoT, забезпечує бездротове підключення на великій площі при низькому споживанні енергії, що дозволяє довготривалу автономну роботу.
- *ZigBee* бездротова мережа для передачі невеликих пакетів даних на короткі відстані, особливо ефективна для домашньої автоматизації та малопотужних пристроїв в промисловості, науці та медицині.
- *Стільникові мережі* пропонують надійну передачу даних та майже глобальне покриття для пристроїв IoT. Стандарти, такі як LTE-M та NB-IoT дозволяють обмін великими обсягами даних або передачу невеликих пакетів через низькочастотні канали.

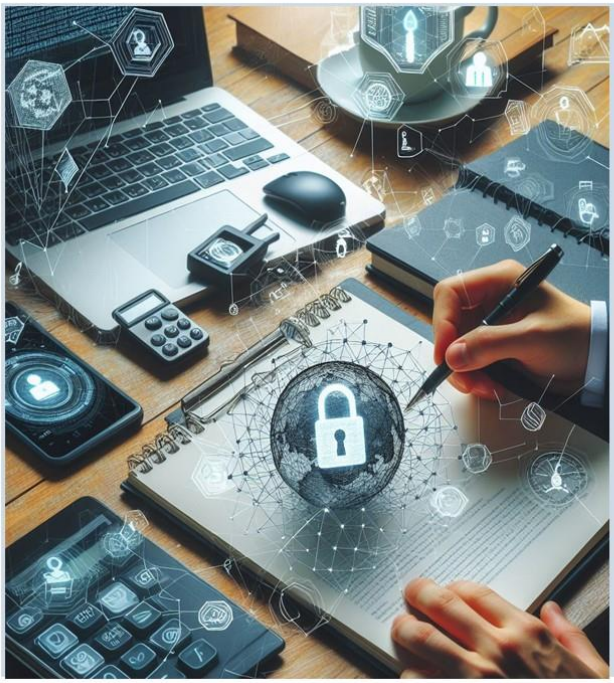




Взаємодія між пристроями та хмарними службами або шлюзами включає в себе використання різноманітних мережевих технологій:

- *Ethernet* використовується для підключення стаціонарних або постійно розташованих пристроїв Інтернету Речей, таких як охоронні та відеокамери.
- *WiFi* найпопулярніша технологія бездротових мереж, ідеально підходить для рішень, які вимагають обробки великих обсягів даних IoT та працюють на обмеженій території.
- NFC (Near Field Communication) забезпечує простий та безпечний обмін даними між двома пристроями на невеликій відстані (10 см або менше).
- *Bluetooth* використовується для зв'язку на короткій відстані, особливо популярний серед переносних пристроїв.

У першому розділі «Аналіз специфікарів архітектурних рівнів для захисту інформації в мережі інтернету речей (IoT)» був проведений аналіз особливостей архітектурних рівнів для забезпечення безпеки інформації в мережі Інтернету речей (IoT). Розглянуті питання визначення актуальності проблеми захисту в IoT, опис архітектури IoT, математичні визначення безпеки систем, а також актуальні виклики інформаційної безпеки в сучасному контексті.



РОЗДІЛ 1.

АНАЛІЗ СПЕЦИФІК АРХІТЕКТУРНИХ РІВНІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

Об'єктом дослідження

Об'єктом дослідження є система захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу.

Предметом дослідження

Предметом дослідження є методики захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу. Вивчення та вдосконалення архітектури мережі IoT для ефективного виявлення та обмеження несанкціонованого доступу.

Метою магістерської роботи

Метою магістерської роботи є проведення докладного дослідження та вивчення методик захисту інформації в мережі Інтернету речей (IoT) від несанкціонованого доступу. Ключовою метою є розробка та вдосконалення стратегій, технологій та методів захисту, спрямованих на забезпечення конфіденційності, цілісності та доступності даних в IoT-системах.

Актуальність теми

Актуальність теми полягає у забезпечення безпеки в мережі Інтернету речей (IoT) від несанкціонованого доступу визначається не лише розширенням самої IoT, але й різноманітністю і значущістю даних, які обробляються цими системами. IoT використовується в різних галузях, включаючи медицину, транспорт, промисловість та побут, і важливо захистити конфіденційні дані, інтегрітету систем і забезпечити доступність сервісів.

Державний університет інформаційно-комунікаційних технологій
Кафедра Інженерії програмного забезпечення автоматизованих систем

ДОСЛІДЖЕННЯ МЕТОДИКИ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖІ ІОТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

на здобуття освітнього ступеня магістра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

ВИКОНАВ: ЗДОБУВАЧ ВИЩОЇ ОСВІТИ ГР. ІСДМ-63
ДАНИЛО КОНДРАТЕНКО
КЕРІВНИК: ОЛЬГА ПОЛОНЕВИЧ

Апробація роботи

Кондратенко Д. В. «Методи захисту інформації в мережі інтернет речей від несанкціонованого доступу: сучасні виклики та рішення». Стаття у загальногалузевому науково-виробничому журналі «Зв'язок», м.Київ - №1, 2024. – С. 234-242
Кондратенко Д. В. «Методи захисту інформації в мережі інтернет речей від несанкціонованого доступу: сучасні виклики та рішення». Тези у науково-практичній конференції «Telecommunication: problems and innovation» – Київ, 16 січня 2024 р.