МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"
УДК 681.3.06

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
“_____” __січня___2022 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛОКАЛЬНОЇ МЕРЕЖІ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ**

Студент групи СЗДМ-61 Ясько Марина Сергіївна _____

Науковий керівник: к.т.н., доцент Котенко Андрій Миколайович _____

Нормоконтроль: Гребенніков Ассаді Болдхоягович _____

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ Г. В. Шуклін
(підпис)
“___”_____ 2022 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Ясько Марині Сергіївні

1. Тема роботи: Підвищення інформаційної безпеки локальної мережі об'єкту інформаційної діяльності

Затверджена наказом по університету “___”_____2021 р. № _____

2. Термін здачі студентом оформленої роботи “___”_____2021 р.

3. Об’єкт дослідження: Процес захисту інформації у локальній мережі об'єкту інформаційної діяльності.

4. Предмет дослідження: . Інформаційна безпека локальної мережі

5. Мета дослідження: Підвищити ефективність інформаційної безпеки локальної мережі об'єкту інформаційної діяльності.

6. Перелік питань, які мають бути розроблені:

1. Загрози інформаційній безпеці у локальних мережах.
2. Аналіз впливу сучасних методів захисту інформації на безпеку локальних мереж об’єктів інформаційної діяльності.
3. Підвищити інформаційну безпеку у локальній мережі об’єкту інформаційної діяльності.

7. Перелік публікацій:

М.С. Ясько. Забезпечення кіберзахисту компьютерної мережі об'єкту інформаційної діяльності. Сучасний захист інформації. Київ: ДУТ, 2021. № 4 (47).

8. Перелік ілюстративного матеріалу:

Презентація на 14 слайдах.

Дата видачі завдання “___”_____ 2021 р.

Науковий керівник _____ А.М. Котенко
(підпис)

Завдання прийнято до виконання _____ М.С. Ясько
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання “___”_____2021 р.

№ з/п	Етапи виконання магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки завдання	16.09.21 р.	Виконано
2.	Аналіз літератури	20.09.21 р.	Виконано
3.	Збір даних	10.10.21 р.	Виконано
4.	Підготовка розділу 1	15.10.21 р.	Виконано
5.	Підготовка розділу 2	11.11.21 р.	Виконано
6.	Підготовка розділу 3	08.12.21 р.	Виконано
7.	Висновки	12.12.21 р.	Виконано
8.	Оформлення презентації	17.12.21 р.	Виконано
9.	Отримання рецензії	24.12.21 р.	Виконано
10.	Захист в ДЕК	.01.22 р.	Виконано

Студент СЗДМ - 61 М.С. Ясько _____

Науковий керівник к.т.н. А.М. Котенко _____

Нормоконтроль: Гребенніков А.Б. _____

РЕФЕРАТ

Дипломна робота містить 78 сторінок, 7 рисунків, 17 джерел, 10 таблиць.

Об’єкт дослідження – Процес захисту інформації у локальній мережі об'єкту інформаційної діяльності.

Предмет дослідження – Інформаційна безпека локальної мережі.

Мета роботи – підвищити ефективність інформаційної безпеки локальної мережі об'єкту інформаційної діяльності.

Методи дослідження – системний аналіз, теорія ймовірності, чисельні методи.

У роботі досліджуються питання підвищення безпеки інформації у локальній мережі об’єкту інформаційної діяльності.

Для підвищення стану інформаційної безпеки проаналізовано існуючий стан справ забезпечення інформаційної безпеки та виявлено проблемні моменти.

Питання забезпечення безпеки інформації у локальній мережі ОІД є комплексним і повинно враховувати фактор безпеки самого ОІД як фізичного середовища.

З урахуванням всього розроблені рекомендації щодо підвищення стану інформаційної безпеки локальної мережі.

Галузь використання – кібербезпека.

Ключові слова: ЛОКАЛЬНА МЕРЕЖА, КОНФІДЕНЦІЙНІСТЬ, МОДЕЛЬ OSI, ЗАГРОЗИ ІНФОРМАЦІЇ, ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА.

ANNOTATION

Thesis contains 80 pages, 7 figures, 17 sources, 10 tables.

Object of Study - The process of protecting information in information systems.

Subject of research - Information security of the local network of the object of information activity.

The purpose of the work is to develop recommendations for improving the state of information security in the local network of the object of activity.

Research methods - system analysis, probability theory, numerical methods.

The paper deals with the issue of improving information security on the local network of the information object.

In order to develop recommendations for improving the state of information security, the existing recommendations were analyzed and problems were identified, namely insufficient consideration of the human factor.

The issue of information security in the local network of the OID is complex and should take into account the security factor of the OID as a physical environment.

Taking into account all the recommendations for improving the information security of the local network.

The area of use is cybersecurity.

Key words: LOCAL NETWORK, CONFIDENTIALITY, OSI MODEL, THREATS OF INFORMATION, TELECOMMUNICATION SYSTEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АСУ – автоматизована система управління

БД – база даних

ЕОМ - електронно-обчислювальна машина

ЗЗІ - засіб захисту інформації

ІБ – інформаційна безпека

ІТС – інформаційно-телекомунікаційна система

ЛОМ – локальна обчислювальна мережа

НСД - несанкціонований доступ

ОІД – об’єкт інформаційної діяльності

ОС - операційна система

ПК - персональний комп’ютер

ВСТУП

У теперішній час неможливо уявити собі серйозну компанію яка не використовує у своїй роботі сучасні інформаційні технології для роботи.

Однією з неодмінних складових даних технологій є об'єднання обчислювальних ресурсів об’єкту інформаційної діяльності у локальну мережу.

Проблема кібернетичної безпеки у інформаційно-телекомунікаційних системах сьогодні дуже гостро стоїть перед організаціями будь-якого рівня. Витік критично важливої інформації, зростання обсягів паразитного трафіку, шантаж і замовні атаки на інформаційні ресурси стали останнім часом частим явищем.

Це обумовлює актуальність теми даної магістерської дисертації, практичне значення якої полягає у розробці конкретних рекомендацій по підвищенню ефективності інформаційної безпеки у локальній мережі об'єкту інформаційної діяльності.

РОЗДІЛ 1
БЕЗПЕКОВІ ФАКТОРИ ЛОКАЛЬНОЇ МЕРЕЖІ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1. Вступ до поняття кібернетичної безпеки

Основна мета концепції кібернетичної безпеки - визначення методів і засобів захисту та забезпечення безпеки інформації, що відповідають інтересам, вимогам і законодавству України в сучасних умовах необхідності використання ресурсів глобальних мереж передачі даних загального користування для побудови корпоративних захищених і безпечних мереж.

Концепція формулює науково-технічні принципи побудови систем забезпечення безпеки інформаційних ресурсів корпоративних мереж з урахуванням сучасних тенденцій розвитку мережевих інформаційних технологій, розвитку видів мережевих протоколів, їх взаємної інкапсуляції та спільного використання.

Основною сучасною тенденцією розвитку мереж зв'язку є їх глобалізація, ускладнення та інтеграція. Інтеграція мережевих і комунікаційних технологій полягає у спільному використанні та інтеграції різноманітних мережевих протоколів, у взаємному використанні комунікаційними провайдерами ресурсів і засобів передачі даних і стикуванні транспортних і сервісних послуг [1], [2].

Ускладнення мережевих технологій пов'язаний з розробкою нових функціональних протоколів зв'язку і передачі інформації, забезпечують більш якісний, і надійний зв'язок, збільшення обсягів і швидкості переданої інформації. Наприклад, для підвищення безпеки передачі інформації був розроблений протокол IPSEC, який входить в нову версію протоколу IPv6.

Тенденція глобалізації визначається необхідністю об'єднання і взаємного використання інформаційних ресурсів, розташованих у віддалених районах і країнах. Ці три основні тенденції розвитку мережевих інформаційних

технологій призводять до четвертої і визначальної тенденції: «Ефективне і гнучке управління безпекою та захистом переданої і оброблюваної інформації засобами централізовано-розподіленого управління».

Ефективна інтеграція неможлива без взаємної довіри і гарантій з безпеки інформації комунікаційних провайдерів. В іншому випадку, інтеграція призводить до фінансових і моральних втрат однієї зі сторін та організаційному руйнування мережі.

Зростання складності комунікаційних технологій призводить до необмеженого росту загроз безпеки інформації, що в умовах відсутності кваліфікованої та гарантованої система забезпечення безпеки інформаційних ресурсів корпоративних мереж призводить до функціонального руйнування мережі.

Глобалізація передбачає різке збільшення числа взаємодіючих суб'єктів обміну інформацією, що при відсутності керованої системи захисту інформації гарантує зворотній від бажаного ефект - гарантії з несанкціонованого доступу і перетворенню цінної для клієнтів інформації в марно перекачуєме інформаційне сміття.

1.2. Загальні питання кібернетичної безпеки об’єкту інформаційної діяльності

Інформаційна безпека має велике значення для забезпечення життєво важливих інтересів будь-якого обєкта інформаційної діяльності. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби.

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд,

повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3].

Втім для практичного використання більш важливою є класифікація інформації за порядком доступу до неї. У відповідності до цього інформація поділяється на: відкриту та з обмеженим доступом (рис. 1.1).

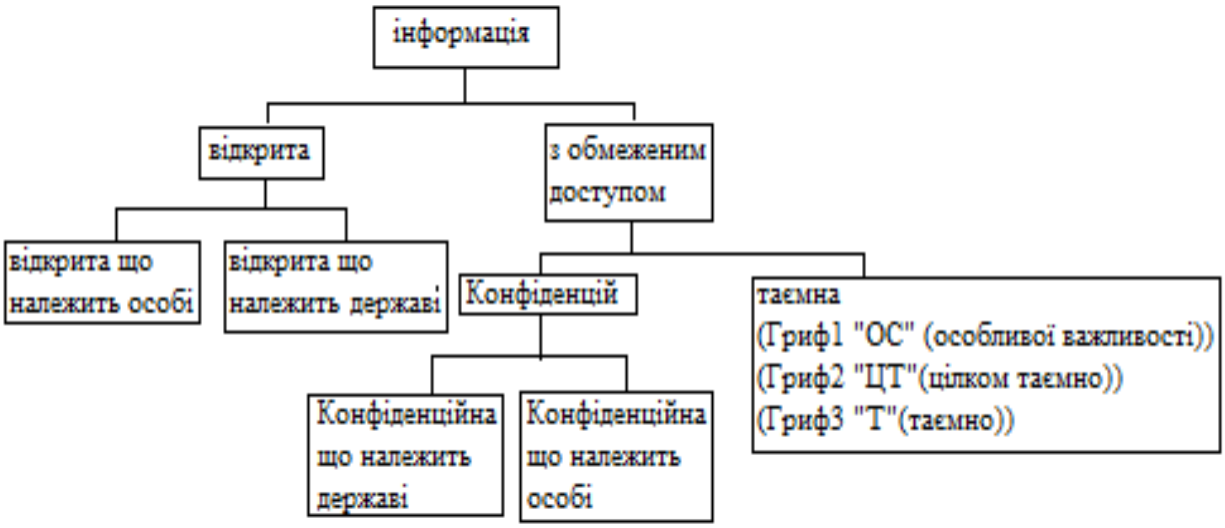

Рисунок 1.1. Розподіл інформації за порядком доступу до неї

У відповідності до Закону "Про захист інформації в інформаційно-телекомунікаційних системах" захисту в системі підлягає:

- відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних

мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);

- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація).

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Усі дії, що пов’язані з обробкою інформації з обмеженим доступом виконуються на об’єктах інформаційної діяльності. Відповідно до визначення об'єкт інформаційної діяльності — будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди функціональне призначення яких передбачає обіг інформації з обмеженим доступом [4]. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на [5]:

–радіоканал;

–електричний;

–акустичний;

–оптичний;

–матеріально-речовий.

Радіоканал (канал передачі даних) — це канал зв'язку, в якому передача інформації здійснюється за допомогою радіохвиль. Включаючи середовище поширення радіохвиль і пристрої перетворення електричних сигналів в електромагнітне випромінювання (радіопередавальний пристрій) та електромагнітне випромінювання в електричні сигнали (радіоприймальний пристрій). Технічні характеристики радіоканалу залежать від його функціонального призначення і виду переданих сигналів: обслуговувана зона, дальність передачі визначають застосовувані частоти, вид антен, потужність передавача і чутливість приймача; вид сигналів (телефонія або телеграфія, звукове або телевізійне мовлення і т. д.) визначає пропускну здатність каналу (смуга переданих частот, динамічний діапазон і лінійність амплітудної характеристики каналу).

Структура радіоелектронного каналу витоку інформації в загальному випадку включає джерело сигналу або передавач, середовище поширення електричного струму або електромагнітної хвилі і приймач сигналу (рис.1.2).

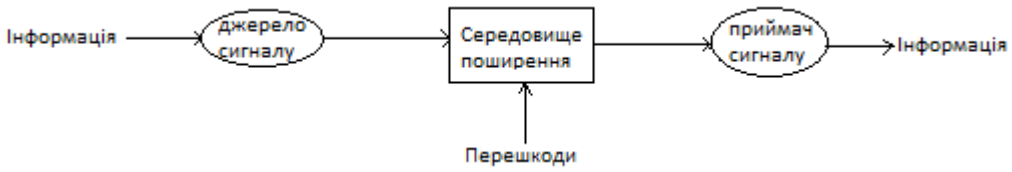

Рис.1.2. Структура радіоелектронного каналу

Особливість радіоканалу полягає в тому, що сигнал вільно випромінюється в ефір, він не замкнутий у кабель, тому виникають проблеми сумісності з іншими джерелами радіохвиль (радіо- і телевіщальними станціями, радарами, радіоаматорськими й професійними передавачами й т.д.). У

радіоканалі використовується передача у вузькому діапазоні частот і модуляцію інформаційних сигналів сигналу несучої частоти. Головним недоліком радіоканалу є його поганий захист від прослуховування, тому що радіохвилі поширюються неконтрольовано. Інший великий недолік радіоканалу - слабка перешкодозахищеність.

Причинами виникнення електричних каналів витоку інформацій можуть бути

– наведення електромагнітних випромінювань ТЗПІ на з'єднувальні лінії

ДТЗС і сторонні провідники, що виходять за межі контрольованої зони;

– просочування інформаційних сигналів у колі електроживлення ТЗПІ;

– просочування інформаційних сигналів у колі заземлення ТЗПІ.

Наведення електромагнітних випромінювань ТЗПІ виникають при випромінюванні елементами ТЗПІ (у тому числі і їх з'єднувальними лініями) інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ТЗПІ і сторонніх провідників або ліній ДТЗС. Рівень сигналів що наводиться, в значній мірі залежить від потужності сигналів що випромінюються, відстані до провідників, а також довжини спільного пробігу з'єднувальних ліній ТЗПІ і сторонніх провідників. Простір навколо ТЗПІ, в межах якого на випадкові антени наводиться інформаційний сигнал вище припустимого (нормованого) рівня, називається (небезпечної) зоною. Випадкової антеною є ланцюг ДТЗС або сторонні провідники, здатні приймати побічні електромагнітні випромінювання. Випадкові антени можуть бути зосередженими і розподіленими. Зосереджена випадкова антена являє собою компактний технічний засіб, наприклад телефонний апарат, гучномовець радіотрансляційної мережі і т.д. До розподілених випадкових антен відносяться випадкові антени з розподіленими параметрами: кабелі, дроти, металеві труби та інші струмопровідні комунікації.

Просочування інформаційних сигналів у коло електроживлення можливо при наявності магнітного зв'язку між вихідним трансформатором підсилювача (наприклад, ПНЧ) і трансформатором випрямляючого пристрою. Крім того, струми інформаційних сигналів що підсилюються, замикаються через джерело електроживлення, створюючи на його внутрішньому опорі падіння напруги, яка при недостатньому загасання у фільтрі випрямляючого пристрою може бути виявлена в лінії електроживлення. Інформаційний сигнал може проникнути в ланцюги електроживлення також в результаті того, що середнє значення споживаного струму в кінцевих каскадах підсилювачів в більшій чи меншій мірі залежить від амплітуди інформаційного сигналу, що створює нерівномірне навантаження на випрямлювач і призводить до зміни споживаного струму за законом зміни інформаційного сигналу.

Одними з найнебезпечніших каналів витоку інформації є акустичні канали. Джерелом утворення акустичного каналу витоку інформації є вібруючі, коливні тіла й механізми, такі як голосовий апарат людини, елементи машин, телефонні апарати, звукопідсилювальні системи тощо.

Канали формуються за рахунок:

– переговорів на відкритому просторі; відкритих вікон, дверей, кватирок, вентиляційних каналів;

– за рахунок будівельних та інженерних особливостей ОІД: стін, стель, підлог, вікон, дверей, коробів, вентиляційних систем, труб водопостачання, систем підігріву та кондиціонування тощо;

– мікрофонного ефекту, акустичної модуляції волоконно-оптичних ліній передачі інформації, ВЧ нав’язування.

1.3. Загрози інформації у локальних мережах

Всі їх можна розділити на дві великі групи: технічні загрози і людський фактор.

Технічні загрози:

- помилки в програмному забезпеченні;
- різні DoS- і DDoS-атаки;
- комп'ютерні віруси, черв'яки, троянські коні;
- аналізатори протоколів і прослуховуючі програми («сніффери»);
- технічні засоби знімання інформації;
- помилки в програмному забезпеченні.

Розглянемо технічні загрози більш детально.

1.3.1. Шкідливе програмне забезпечення та шкідливий код

Віруси

Вірус - це шкідливий програмний код, прикріплений до виконуваного файлу, наприклад, легітимної програми [8]. Для більшості вірусів необхідно, щоб користувач запустив заражену програму, також вони можуть активуватися в конкретний час або дату. Комп'ютерні віруси зазвичай поширюються одним із трьох способів: через знімні носії; завантажуються з Інтернету; через вкладення електронної пошти. Віруси можуть бути нешкідливими і просто виводити рисунок на екран, або можуть бути руйнівними, як наприклад ті, що змінюють або видаляють дані. Щоб уникнути виявлення, вірус мутує. Комп'ютер може бути заражений вірусом просто в результаті того, що користувач відкрив файл. Деякі віруси вражають завантажувальний сектор або файлову систему флеш-накопичувачів USB, а з них можуть поширюватися на системний жорсткий диск комп’ютера. Також зараження вірусами може відбуватися при виконанні конкретної програми. Після активації вірусу він постійно заражатиме інші програми на комп'ютері або на інших комп'ютерах в мережі. Вірус Меліса став прикладом вірусу, який поширювався електронною поштою. Меліса завдала

шкоди десяткам тисяч користувачів і, за приблизними оцінками, спричинила збитків на 1.2 мільярда доларів.

Черв'яки.

Черв'яки - це зловмисний код, який поширюється самостійно, використовуючи вразливості мережної інфраструктури [8]. Зазвичай черв'яки уповільнюють роботу мережі. На відміну від вірусів, які потребують запуску зараженої програми-носія, черв'яки можуть працювати самостійно. Після первинного інфікування черв'яки більше не потребують участі користувача. Після зараження вузла черв'як може швидко поширюватися мережею. Черв'яки діють за єдиним принципом. Всі вони використовують певну вразливість, мають механізм розповсюдження і виконують певну зловмисну дію.

Черв'яки відповідальні за деякі найбільш руйнівні атаки в Інтернеті. Наприклад, в 2001 році черв'як Code Red інфікував 658 серверів. За 19 годин цей черв'як заразив більше ніж 300 тисяч серверів.

Троянський кінь.

Троянський кінь (троян) - це зловмисне програмне забезпечення, яке здійснює шкідливі дії під виглядом бажаної операції, наприклад онлайн-гри [5]. Цей шкідливий код використовує привілеї користувача, який його запускає. Троянський кінь відрізняється від віруса тим, що прив'язується до невиконуваних файлів, таких як файли зображень, аудіофайли або ігри.

Логічна бомба.

Логічна бомба - це шкідлива програма, яка використовує тригер (активатор) для пробудження шкідливого коду. Наприклад, активатором може бути дата, час, запуск інших програм, або видалення облікового запису користувача. Логічна бомба залишається неактивною, доки не відбудеться подія, що активує цей код. Після активації логічна бомба виконує зловмисний код, який завдає шкоди комп'ютеру. Цей тип зловмисного ПЗ може пошкодити записи в базі даних, видалити файли та атакувати операційні системи або застосунки. Нещодавно фахівці з кібербезпеки виявили новий тип логічних

бомб, які атакують та руйнують апаратні компоненти робочих станцій та серверів, а саме вентилятори охолодження, процесор, пам'ять, жорсткі диски та блоки живлення. Логічна бомба примушує ці пристрої працювати в критичному режимі, доки вони не перегріються або не вийдуть з ладу.

Backdoor.

Термін backdoor (чорний хід) відноситься до програми або коду, доданого зловмисником, який скомпроментував систему [6]. Backdoor обходить стандартну аутентифікацію, яка використовується для доступу до системи. До найбільш поширених програм цього типу відносяться Netbus і Back Orifice, що надають віддалений доступ до системи неавторизованим користувачам. Мета backdoor - надавати кібер-злочинцям доступ до системи в майбутньому, навіть після того, як організація виправить вразливість, яка була використана для атаки на систему. Зазвичай, щоб встановити backdoor, злочинці використовують авторизованих користувачів, які несвідомо запускають троянську програму на своєму ПК.

Руткіт.

Руткіт (Rootkit) модифікує операційну систему для створення чорного ходу. Потім зловмисники використовують backdoor для віддаленого доступу до комп'ютера. Більшість руткітів використовують вразливості програмного забезпечення для підвищення рівня привілеїв (ескалації прав доступу) та модифікації системних файлів. Ескалація привілеїв можлива через помилки програмування або недоліки проектування і дозволяє зловмисникам отримати підвищений рівень доступу до мережних ресурсів та даних. Також руткіти здійснюють зміни в системи перевірки стану та інструментах моніторингу, що дуже ускладнює виявлення зловмисного ПЗ такого типу. Часто для знищення руткіту доводиться перевстановити операційну систему.

Атаки через браузер та електронну пошту.

Електронна пошта - це універсальний сервіс, що використовується мільярдами людей у всьому світі. Як один з найбільш популярних сервісів, електронна пошта стала головною вразливістю для користувачів та організацій.

Спам.

Спам, також відомий як небажана пошта, або небажаний електронний лист [5]. У більшості випадків спам - це один зі способів реклами. Однак спам може містити небезпечні посилання, зловмисне ПЗ або оманливий вміст. Кінцевою метою такого спаму є отримання конфіденційної інформації користувача, такої як номер соціального страхування або інформація про банківський рахунок. Більшість спаму надходить з великої кількості комп'ютерів, які розташовані в мережах, заражених вірусом або Інтернет-черв'яком. Ці скомпрометовані комп'ютери надсилають максимально можливу кількість повідомлень електронної пошти. Характерні признаки спаму: в електронному листі відсутня тема, електронний лист вимагає оновлення облікового запису, текст електронного листа містить слова з помилками або дивну пунктуацію, посилання в електронному листі є довгими та/або незрозумілими, електронний лист виглядає як листування з реально існуючою організацією, електронний лист вимагає від користувача відкрити вкладення.

Якщо користувач отримує електронний лист, що відповідає одному або декільком з цих характеристик, йому не варто відкривати цей лист або будь-які вкладення. Зазвичай політика використання електронної пошти організації вимагає, щоб користувач, який отримав електронний лист такого типу, повідомив про це співробітникам відділу кібербезпеки. Майже всі поштові сервіси фільтрують спам. На жаль, спам все одно створює навантаження на мережу і сервер отримувача.

Шпигунське програмне забезпечення.

Шпигунське ПЗ - це програмне забезпечення, яке дозволяє злочинцям отримувати інформацію про дії користувача за комп'ютером. Шпигунські програми часто містять засоби відстеження активності, набраних на клавіатурі

символів та перехоплення даних. Для того, щоб обійти заходи безпеки, шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто прив'язуються до легального ПЗ або розповсюджуються троянами. Багато веб-сайтів, які поширюють умовно-безкоштовні програми (shareware), містять шпигунські програми. Рекламне ПЗ зазвичай відображає надокучливі спливаючі вікна з метою отримання доходу їх авторами від реклами. Зловмисне програмне забезпечення може аналізувати інтереси користувача, відстежуючи які веб-сайти він відвідує. Потім зловмисне ПЗ може надсилати спливаючу рекламу, яка відповідає тематиці цих сайтів. Деякі версії програмного забезпечення автоматично встановлюють рекламне ПЗ. Деяке рекламне ПЗ дійсно забезпечує тільки доставку реклами, але часто рекламне ПЗ поширюється разом зі шпигунським. **Scareware** - це шкідливе ПЗ, яке переконує користувача здійснити конкретну дію, використовуючи його страх. Scareware створює спливаючі вікна, схожі на вікна діалогу операційної системи. Ці вікна містять підроблені повідомлення про те, що система знаходиться під загрозою або необхідно виконання певної програми для повернення до нормальної роботи. Насправді жодних проблем немає і якщо користувач дозволить виконати зазначену програму, вона встановить на його комп'ютер зловмисний код.

Фішинг.

Фішинг - це форма шахрайства. Кіберзлочинці, маскуючись під організацію чи особу з гарною репутацією, використовують електронну пошту, системи миттєвого обміну повідомленнями або соціальні мережі для збору такої інформації, як реєстраційні дані або дані облікового запису. Фішинг відбувається, коли зловмисник надсилає шахрайського електронного листа, який виглядає як такий, що надійшов з надійного джерела. Мета цього повідомлення - змусити одержувача встановити зловмисне програмне забезпечення на своєму пристрої або повідомити персональну чи фінансову інформацію. Прикладом фішингу є фальшивий електронний лист начебто від

магазину. В цьому листі користувачу пропонують перейти за посиланням, щоб отримати приз. За цим посиланням користувач переходить на підроблену веб-сторінку, яка запитує персональну інформацію, або встановлює вірус. *Спрямований фішинг (spear phishing)*- це цілеспрямована фішингова атака. Як звичайний, так і спрямований фішинг використовують електронну пошту, щоб досягнути жертв. Але у випадку спрямованого фішингу персоналізовані електронні листи надсилають конкретній особі. **Голосовий фішинг (Vishing)** - це фішинг за допомогою технологій голосових комунікацій. Злочинці можуть робити фальшиві дзвінки, представляючись довіреними організаціями, за допомогою технології передачі голосу через IP (VoIP). Жертви також можуть отримати записане повідомлення, яке виглядає легітимним. Таким чином злочинці намагаються отримати номери кредитних карток або іншу інформацію, щоб викрасти персональні дані жертви. **СМС фішинг (Smishing)** – це вид фішингу, який використовує текстові повідомлення на мобільних телефонах. Злочинці видають себе за офіційне джерело щоб завоювати довіру жертви. Наприклад, під час СМС фішингу зловмисник може надіслати жертві посилання на веб-сайт. Коли жертва відвідає цей веб-сайт, на мобільний телефон буде встановлене зловмисне ПЗ. **Фармінг (pharming)** - це фальшивий веб-сайт, що має вигляд справжнього, щоб змусити користувачів вводити свої облікові дані. Під час фармінгу користувачів спрямовують на фальшивий веб-сайт, який імітує офіційний. Потім жертви вводять свою особисту інформацію, вважаючи, що вони підключені до легітимного сайту. **Whaling** (полювання на корпоративних китів)- це фішингова атака, що спрямована на осіб, які мають повний доступ до інформації у межах організації, наприклад, її вище керівництво. Також цілями можуть бути політики або знаменитості.

Зараження браузерів та підключаємих модулів.

Зловмисники заражують веб-браузери з метою їх використання для відображення спливаючої реклами, збору особистої інформації або встановлення рекламного ПЗ, вірусів, шпигунських програм. Зловмисний код

може бути встановлений у виконуваний файл браузера, компоненти браузера або його плагіни [10].

Плагіни.

Плагіни Flash та Shockwave від Adobe дозволяють створювати цікаві графічні та мультиплікаційні зображення, які значно покращують зовнішній вигляд веб-сторінки. Плагіни відображають контент, створений за допомогою відповідного програмного забезпечення. До недавнього часу плагіни мали дивовижно рекордні показники з точки зору безпеки. Однак з ростом популярності контенту на основі Flash, зловмисники звернули увагу на плагіни та програмне забезпечення Flash, визначили вразливі місця та змогли використати їх у своїх цілях. Успішна атака може викликати збій системи або дозволить зловмисникам взяти її під свій контроль. Прогнозується збільшення втрат даних, оскільки злочинці продовжують досліджувати найбільш популярні плагіни та протоколи у пошуках вразливостей.

Browser Hijacker (Викрадач браузерів).

Викрадач браузерів - це зловмисне ПЗ, яке змінює налаштування веб-браузера на комп'ютері з метою перенаправлення користувача на проплачені веб-сайти. Викрадачі браузерів зазвичай встановлюються без дозволу користувача під час прихованого завантаження (drive-by download). Прихованим завантаженням називають програму, яка автоматично завантажується на комп'ютер, коли користувач відвідує певний веб-сайт або переглядає електронний лист в HTML. Завжди уважно читайте користувацькі угоди, коли завантажуєте програми, щоб уникнути загроз такого типу.

1.3.2. Кібератаки

"Відмова в обслуговуванні" (DoS)

Атака типу "Відмова в обслуговуванні" (DoS) - є різновидом мережної атаки. Результатом DoS-атаки є переривання доступу користувачів, пристроїв або застосунків до мережних сервісів [6]. Існує два основних типи DoS-атак:

Перевантаження великою кількістю трафіку - Нападник надсилає величезну кількість даних з такою швидкістю, що мережа, хост або застосунок не встигає їх обробляти. Це спричиняє уповільнення передачі або реагування, іноді призводить до аварійного завершення роботи пристрою чи сервісу.

Пакети неправильного формату (Maliciously Formatted Packets) - Нападник надсилає пакет даних неправильного формату хосту або застосунку і одержувач не може його обробити. Наприклад, програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані. Це призводить до того, що приймаючий пристрій буде працювати дуже повільно або припинить роботу взагалі.

DoS-атаки становлять серйозний ризик, оскільки вони можуть легко переривати обмін інформацією та заподіяти значну втрату часу й грошей. Ці атаки відносно прості для виконання навіть некваліфікованим нападником. Метою атаки «відмова в обслуговуванні» є припинення доступу для авторизованих користувачів через недоступність мережної інфраструктури (згадайте три основні принципи безпеки: конфіденційність, цілісність та доступність).

Розподілена *DoS атака (DDoS)* подібна до атаки DoS, але вона походить з декількох скоординованих джерел [12]. Наприклад, атака DDoS може розвиватися наступним чином. Зловмисник створює мережу заражених хостів, яка називається ботнетом і складається з комп'ютерів-зомбі. Зомбі - це заражені хости. Для контролю над зомбі зловмисник використовує спеціальну керуючу систему. Комп'ютери-зомбі постійно сканують мережу і заражають інші хости, створюючи ще більше нових зомбі. Після такої підготовки хакер через керуючу систему дає наказ ботнету розпочати DDoS атаку.

Аналіз трафіку (Sniffing)

Sniffing є дуже схожим на підглядання за людиною в реальному світі. Хакери досліджують весь мережний трафік, який проходить через їх мережну інтерфейсну карту (NIC), незалежно від того, кому він адресований. Злочинці

виконують аналіз трафіку в мережі за допомогою програмного забезпечення, апаратного пристрою або їх комбінації. Як показано на рисунку, Sniffing переглядає весь мережний трафік або виконується фільтрація за певним протоколом, сервісом чи навіть за рядком символів, таких як ідентифікатор користувача або пароль. Деякі мережні аналізатори можуть перевіряти весь трафік і навіть змінювати його частково або повністю. Sniffing може бути корисним. Мережні адміністратори можуть використовувати такі засоби для аналізу мережного трафіку, визначення проблем з пропускною здатністю та вирішення інших проблем в мережній інфраструктурі. Фізична безпека має важливе значення для запобігання встановленню аналізаторів трафіку у внутрішній мережі організації.

Підміна (Spoofing)

Підміна (Spoofing) – це атака шляхом імперсоніфікації, яка відбувається за рахунок використання довірчих відносин між двома системами [12]. Якщо дві системи підтримують єдину аутентифікацію, користувач, який увійшов до однієї системи, може не проходити повторно процес аутентифікації для доступу до іншої системи. Зловмисник може скористатися цими довірчими відносинами, відправивши пакет до однієї системи, який виглядає як такий, що надійшов з іншої довіреної системи. Оскільки між системами діють довірчі відносини, цільова система може виконати запит без аутентифікації.

Існує кілька типів атак з використанням підміни:

підміна MAC-адреси відбувається, коли один комп'ютер приймає пакети даних, адресовані на MAC-адресу іншого комп'ютера;

IP-spoofing надсилає IP-пакети з підробленої IP-адреси джерела, щоб замаскувати свою справжню адресу;

протокол визначення адрес (ARP) - це протокол, який перетворює IP-адреси в MAC-адреси для передачі даних. При ARP підміні зловмисник розсилає підроблені ARP повідомлення локальною мережею для того, щоб зв'язати свою MAC-адресу з IP-адресою авторизованого користувача мережі.

система доменних імен (DNS) асоціює доменні імена з IP-адресами. При підміні DNS відбувається модифікація DNS-сервера для перенаправлення певного доменного імені на іншу IP-адресу, контрольовану злочинцем.

Клавіатурний шпигун (keylogger)/

Клавіатурний шпигун (кеqлогер) - це програма, яка записує або вносить в спеціальний журнал натискання клавіш користувачем системи. Злочинці можуть реалізовувати кейлогери за допомогою ПЗ, встановленого на комп'ютері або через обладнання, фізично приєднане до комп'ютера. Зловмисник налаштовує ПЗ клавіатурного шпигуна таким чином, щоб воно відправляло зібрану в журналі інформацію електронною поштою. Перехоплені та записані до лог-файлу натискання клавіш можуть розкрити імена користувачів, паролі, відвідані веб-сайти та іншу конфіденційну інформацію. Клавіатурні шпигуни можуть бути легальними, комерційними програмами. Хоча кейлогери не є незаконними програмами, але злочинці використовують їх для досягнення своїх незаконних цілей.

До людського фактору відносяться:

Звільнені або незадоволені співробітники.

Промислове шпигунство.

Халатність.

Низька кваліфікація.

1.4. Критерії інформаційної безпеки локальної мережі

Фахівці з кібербезпеки - це експерти, які займаються захистом у кіберпросторі. Джон Мак-Камбер один з перших експертів з кібербезпеки, розробив широко використовувану конструкцію під назвою Куб Мак-Камбера або Куб кібербезпеки. Він використовується як інструмент для захисту мереж, доменів та Інтернету [6].

Перший вимір Куба кібербезпеки визначає три принципи інформаційної безпеки. Фахівці з кібербезпеки називають ці три принципи (конфіденційність, цілісність, доступність) КЦД-тріадою (CIA Triad). Другий вимір визначає три стани інформації або даних. Третій вимір куба визначає необхідні дії для забезпечення захисту. Ці виміри часто називають трьома категоріями гарантованої кібербезпеки. Розглянемо модель кібербезпеки ISO. Вона являє собою міжнародну основу стандартизації та керування інформаційними системами.

Принципи захисту. Перший вимір куба кібербезпеки визначає цілі захисту кіберпростору. Цілі, визначені в першому вимірі, є основоположними принципами. Цими трьома принципами є конфіденційність, цілісність і доступність. Ці принципи забезпечують орієнтир і дозволяють фахівцеві з кібербезпеки визначати пріоритети дій при захисті будь-якої мережної системи Конфіденційність запобігає розкриттю інформації неавторизованим людям, ресурсам або процесам. Цілісність даних позначає їх точність, узгодженість та достовірність. Нарешті, доступність гарантує, що інформація доступна авторизованими користувачами у разі потреби. Для запам’ятовування цих трьох принципів використовуйте абревіатуру КЦД (англ. CIA).

Стани даних. Кіберпростір - це домен, що містить значну кількість критично важливих даних. Тому експерти з кібербезпеки зосереджені на захисті даних. Другий вимір куба кібербезпеки зосереджений на проблемах захисту даних, які знаходяться у кіберпросторі в різних станах. Дані мають три можливі стани:

- Дані в передачі
- Дані в стані спокою або зберігання
- Дані в обробці

Захист кіберпростору вимагає, щоб фахівці в області кібербезпеки гарантували безпеку даних у всіх трьох станах.

Контрзаходи. Третій вимір куба кібербезпеки визначає навички і знання, які фахівець з кібербезпеки може використовувати для захисту у кіберпросторі. Фахівці з кібербезпеки повинні використовувати цілу низку наявних навичок і знань, коли захищають дані в кіберпросторі. Вони повинні це робити залишаючись при цьому на стороні закону.

Куб кібербезпеки визначає три типи навичок, які використовуються для забезпечення захисту. Перша навичка включає в себе технології, пристрої та продукти для захисту інформаційних систем і запобігання діям кіберзлочинців. Фахівці з кібербезпеки повинні володіти спеціалізованими технологічними інструментами. Проте, Мак-Камбер нагадує їм, що для перемоги над кіберзлочинцями недостатньо самих лише технологічних засобів. Професіонали з кібербезпеки також повинні вибудовувати потужний захист через налаштування політик, процедур та рекомендацій, які дозволяють користувачам кіберпростору залишатися у безпеці та дотримуватися принципів передової практики. Нарешті, користувачі кіберпростору повинні прагнути більшої обізнаності щодо загроз у кіберпросторі та виробити культуру навчання та усвідомлення у сфері інформаційної безпеки [7].

Конфіденційність запобігає розкриттю інформації неавторизованим особам, ресурсам або процесам. Синонімом конфіденційності є приватність. Організації обмежують доступ, щоб гарантувати, що тільки уповноважені оператори можуть використовувати дані або інші мережні ресурси. Наприклад, програміст не повинен мати доступ до особистої інформації всіх співробітників.

Організації повинні навчати співробітників кращим методам захисту конфіденційної інформації, щоб захистити їх та себе від атак. Методи, які використовуються для забезпечення конфіденційності, включають шифрування даних, аутентифікацію і контроль доступу.

Контроль доступу визначає ряд схем захисту, які запобігають несанкціонованому доступу до комп'ютера, мережі, бази даних або інших

ресурсів даних. Концепція ААО (англ. AAA) включає в себе три служби безпеки: аутентифікація, авторизація та облік. Ці служби забезпечують основну структуру контролю доступу.

Перше «А» в ААО (ААА) позначає аутентифікацію. Аутентифікація перевіряє особу користувача для запобігання несанкціонованому доступу. Користувачі підтверджують свою особистість за ім'ям користувача або ідентифікатором. Окрім того, користувачі повинні підтвердити свою особу за одним із способів:

надати інформацію яку вони знають (наприклад, пароль);

підтвердити наявність чогось (наприклад, токен або картка);

надати біометричну інформацію (наприклад, відбитки пальців).

Авторизація, визначає через свою службу до яких ресурсів можуть отримати доступ користувачі, а також операції, які вони можуть виконувати. Деякі системи реалізують це за допомогою списку керування доступом або ACL (англ. Access Control List). ACL визначає, чи має користувач певні привілеї доступу після проходження аутентифікації. Авторизація також може контролювати, коли користувач має доступ до певного ресурсу. Наприклад, співробітники можуть мати доступ до бази даних продажів в робочий час, але система блокує їх у неробочий час.

Облік, відстежує дії користувача, а саме, до яких даних вони зверталися, тривалість використання ресурсів та будь-які зроблені зміни. Наприклад, банк відстежує облікові записи кожного клієнта. Аудит цієї системи може виявити час і кількість всіх транзакцій, а також співробітника або системи, які виконували транзакції. Служби обліку кібербезпеки працюють так само. Система відстежує кожну транзакцію даних і надає результати аудиту.

Цілісність - це точність, узгодженість і достовірність даних протягом всього життєвого циклу. Іншими словами цілісність - це якість. Дані повинні залишатися незмінними під час виконання всіх цих операцій неавторизованими суб'єктами. Методи, які використовуються для забезпечення цілісності даних,

включають хешування, перевірку достовірності даних, перевірку узгодженості даних і керування доступом. Системи цілісності даних можуть включати один або декілька методів, наведених вище. Перевірка цілісності - це спосіб вимірювання узгодженості набору даних (файлу, зображення або записів). Перевірка цілісності виконується за допомогою такого процесу як хеш-функції для миттєвого формування відбитку даних. Перевірка цілісності використовує цей відбиток аби переконатися, що дані залишилися незмінними. Контрольна сума є одним із прикладів хеш-функції. Контрольна сума підтверджує цілісність файлів або рядків символів до і після їх передачі з одного пристрою на інший через локальну мережу або Інтернет. Контрольна сума просто перетворює кожну частину інформації в значення і підсумовує їх. Щоб перевірити цілісність даних, система, яка отримала файл, повторює цей процес. Якщо дві суми рівні, дані дійсні, якщо вони не рівні, десь в процесі передачі відбулася зміна. На сьогоднішній день популярні такі хеш-функції як MD5, SHA-1, SHA-256 і SHA-512. Ці хеш-функції використовують складні математичні алгоритми. Значення хешу використовується для порівняння.

Доступність даних - це принцип, який використовується для опису необхідності постійно підтримувати доступність інформаційних систем і послуг. Кібератаки і збої системи можуть перешкоджати доступу до інформаційних систем і служб. Наприклад, перериванням доступності веб-сайту шляхом виведення його з ладу можуть скористатися конкуренти. Ці атаки типу «відмова в обслуговуванні» (DoS) загрожують доступності системи і не дозволяють користувачам отримувати доступ до інформаційних систем і використовувати їх при необхідності. Методи, які використовуються для забезпечення доступності, включають системне резервування, резервне копіювання системи, підвищену відмовостійкість системи, технічне обслуговування обладнання, сучасні операційні системи та програмне забезпечення і плани по швидкому відновленню від непередбачених лих.

Організації можуть забезпечити доступність, регулярно виконуючи такі дії:

обслуговування обладнання;

оновлення ОС та системи;

резервне копіювання;

планування дій на випадок стихійних лих;

нові технологічні реалізації;

моніторинг надзвичайної активності;

перевірка доступності.

Висновок по розділу. Безпека інформації ЛОМ ОІД складається з безпосередньо з мережевої безпеки та безпеки самого ОІД. Описано мережеві загрози інформації у ЛОМ та загрози витоку інформації з ОІД. Визначені критерії інформаційної безпеки

РОЗДІЛ 2
ШЛЯХИ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ ОІД

2.1. Технічна безпека інформації локальній у мережі

Захист від зловмисного ПЗ

Кілька простих кроків допоможуть захистити ваш комп'ютер від усіх видів зловмисного програмного забезпечення.

Антивірусна программа. Більшість антивірусних пакетів успішно виявляють найпоширеніші форми шкідливого ПЗ. Проте щоденно кіберзлочинці розробляють і розповсюджують нові загрози. Тому ключем до ефективного захисту проти вірусів є постійне оновлення бази вірусних сигнатур. Сигнатура для віруса - це як відбиток пальця для людини. Вона ідентифікує характерні елементи зловмисного коду, за якими його можна розпізнати [8].

Актуальне ПЗ. **Б**агато форм зловмисного ПЗ досягають своїх цілей через використання вразливостей програмного забезпечення як в операційних системах, так і в застосунках. Раніше вразливості операційної системи були основним джерелом проблем, на сьогоднішній день найбільший ризик становлять вразливості застосунків. В той час, як розробники операційних систем все швидше реагують на нові загрози, більшість розробників прикладного ПЗ на жаль нехтують цим.

Захист від атак через браузер та електронну пошту.

Методи боротьби зі спамом включають фільтрування електронної пошти, навчання користувачів щодо обережного ставлення до підозрілих електронних листів та використання фільтрів на хостах/серверах. Важко зупинити спам повністю, але можна зменшити його наслідки. Наприклад, більшість інтернет-

провайдерів блокують спам, перш ніж він потрапить до поштової скриньки користувача. Більшість антивірусів та поштових клієнтів автоматично виконують фільтрацію електронних листів. Це означає, що вони виявляють та видаляють спам з електронної поштової скриньки користувача. Організації також повинні попереджати працівників про небезпеку відкривання вкладень електронної пошти, які можуть містити віруси або Інтернет-черв'яки. Не вважайте, що вкладення електронної пошти є безпечними, навіть якщо вони надійшли від надійного джерела. Комп'ютер відправника може без його відому використовуватися для розповсюдження вируса. Завжди перевіряйте вкладення електронної пошти перед тим, як їх відкрити.

Антифішингова робоча група (APWG) - це галузева асоціація з протидії викраданню особистих даних та шахрайствам, які виникають в результаті фішингу або підробки електронних листів. Регулярне оновлення всього програмного забезпечення гарантує, що в системі є всі найновіші виправлення безпеки для усунення відомих вразливостей.

Захист від кібератак.

Організація може запровадити низку заходів для захисту від різноманітних атак. Налаштуйте міжмережні екрани так, щоб відхиляти будь-які пакети, що надходять ззовні мережі, але мають адреси, які вказують на їх походження з внутрішньої мережі. Така ситуація є незвичайною, і це вказує на те, що кібер-злочинець спробував здійснити атаку з підміною адреси. Щоб запобігти DoS та DDoS атакам, переконайтеся, що патчі та оновлення є актуальними, розподіляйте навантаження між серверними системами та блокуйте зовнішні ICMP пакети на межі периметру. Мережні пристрої використовують ICMP-пакети для надсилання повідомлень про помилки. Наприклад, команда ping використовує ICMP пакети для перевірки чи може пристрій взаємодіяти з іншими пристроями в мережній інфраструктурі. Системи можуть попередити повторні напади, шифруючи трафік,

використовуючи криптографічну аутентифікацію та включаючи часові мітки до кожної частини повідомлення.

2.2. Шляхи підвищення ефективності захисту інформації у локальный мережі

Для підвищення ефективності захисту інформації необхідно враховувани усі види загроз що здатні завдати шкоди підприємству(організації), детальний пререрахунок загроз було наведено у розділі 1.2, та вдосконалювати вже існуючі методи захисту , або вживати заходів що до впровадження нових або більш сучасних методів. Також потрібно розуміти, що кількість загроз постійно зростає, з'являються все нові і нові віруси, збільшується інтенсивність і частота DDoS-атак. Це безумовно складає труднощі для організації вконання вимог інформаційної безпеки, захисту інформації в тому числі захисту від несанкціонованого доступу до засобів обчислювальної техніки [10].

Тому, для запобігання можливості появи загроз ІБ і ЗІ в організаціях роблять комплекс різних заходів, впроваджують різні методи (більш детально розглянемо нижче), які умовно можна розділити на технічні, правові та заходи розмежування доступу.

До методів і засобів організаційної захисту інформації відносяться організаційно-технічні та організаційно-правові заходи, що проводяться в процесі створення і експлуатації КС для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, в яких будуть розміщуватися комп'ютери; проектуванні системи, монтажі та налагодження її технічних і програмних засобів; випробуваннях і перевірці працездатності комп'ютерної системи.

Основою проведення організаційних заходів є використання і підготовка законодавчих і нормативних документів в області інформаційної безпеки, які на правовому рівні повинні регулювати доступ до інформації з боку споживачів.

Інженерно-технічний захист (ІТЗ) - це сукупність спеціальних органів, технічних засобів і заходів по їх використанню в інтересах захисту конфіденційної інформації.

Різноманіття цілей, завдань, об'єктів захисту і заходів, що проводяться передбачає розгляд певної системи класифікації засобів за видом, орієнтації та інші характеристики. Наприклад, кошти інженерно-технічного захисту можна розглядати по об'єктах їх впливу. В цьому плані вони можуть застосовуватися для захисту людей, матеріальних засобів, фінансів, інформації [11].

Різноманіття класифікаційних характеристик дозволяє розглядати інженерно-технічні засоби по об'єктах впливу, характером заходів, способам реалізації, масштабом охоплення, класу засобів зловмисників, яким чиниться протидія з боку служби безпеки.

За функціональним призначенням кошти інженерно-технічного захисту діляться на наступні групи:

1. матеріальні ресурси, що включають різні засоби і споруди, що перешкоджають фізичному проникненню (або доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації і здійснюють захист персоналу, матеріальних засобів, фінансів та інформації від протиправних дій;

2. апаратні засоби - прилади, пристрої, пристосування і інші технічні рішення, які використовуються в інтересах захисту інформації. У практиці діяльності підприємства знаходить широке застосування найрізноманітніша апаратура, починаючи з телефонного апарату до скоєних автоматизованих систем, що забезпечують виробничу діяльність. Основне завдання апаратних засобів - забезпечення стійкої захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності;

3. програмні засоби, що охоплюють спеціальні програми, програмні комплекси і системи захисту інформації в інформаційних системах різного

призначення і засобах обробки (збір, накопичення, зберігання, обробка і передача) даних;

4. криптографічні засоби - це спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по системам і мережам зв'язку, зберігається та обробляється на ЕОМ з використанням різноманітних методів шифрування.

Фізичні засоби захисту - це різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників.

До фізичних засобів належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні та інші пристрої для заборони несанкціонованого доступу (входу, виходу), проносу (виносу) коштів і матеріалів та інших можливих видів злочинних дій.

Ці засоби застосовуються для вирішення наступних завдань:

- охорона території підприємства і спостереження за нею;
- охорона будинків, внутрішніх приміщень та контроль за ними;
- охорона обладнання, продукції, фінансів та інформації;
- здійснення контрольованого доступу в будівлі і приміщення.

Всі фізичні засоби захисту об'єктів можна розділити на три категорії: засоби попередження, засоби виявлення і системи ліквідації загроз. Охоронна сигналізація і охоронне телебачення, наприклад, відносяться до засобів виявлення загроз; паркани навколо об'єктів - це засоби попередження несанкціонованого проникнення на територію, а посилені двері, стіни, стелі, решітки на вікнах та інші заходи служать захистом і від проникнення, і від інших злочинних дій (підслуховування, обстріл, кидання гранат і вибухових пакетів і т. д .). Засоби пожежогасіння відносяться до систем ліквідації загроз.

До апаратних засобів захисту інформації відносяться найрізноманітніші за принципом дії, влаштування та можливостям технічні конструкції, що

забезпечують припинення розголошення, захист від витоку і протидія несанкціонованому доступу.

Найголовнішим методом є комплексна система захисту інформації основною проблемою реалізації якої є:

– з одного боку, забезпечення надійного захисту, що знаходиться в системі інформації: виключення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації і про обслуговуючого персоналу;

– з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякою сукупністю наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів по ЗІ .

На основі теоретичних досліджень і практичних робіт в області ЗІ сформульований системно-концептуальний підхід до захисту інформації.

Під системністю як основною частиною системно-концептуального підходу розуміється:

– системність цільова - захищеність інформації розглядається як основна частина загального поняття якості інформації;

– системність просторова, яка пропонує взаємопов'язані рішення всіх питань захисту на всіх компонентах підприємства;

– системність тимчасова, що означає безперервність робіт по ЗІ, що здійснюються відповідно до планів;

– системність організаційна, що означає єдність організації всіх робіт по ЗІ і управління ними [12].

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт по ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи включає в себе: перш за все, вивчення об'єкта впроваджуваної системи; оцінку загроз безпеки об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх чинників; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця.

Комплексний (системний) підхід - це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені наступні її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. В якості вхідних елементів виступають види загроз безпеки, можливі на даному об'єкті;

2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. Д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими

об'єктами. Дуже важливо встановити межі області інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій по захисту інформації, переданої сигналами в кабельної лінії, що проходить по територіях різних об'єктів. Як би не встановлювалися кордону системи, не можна ігнорувати її взаємодія з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними. Це справедливо як для кордонів, що захищається, так і для кордонів системи захисту;

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей (підцілей). Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декількох варіантів побудови системи, що забезпечує задані цілі функціонування. Для того щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з

основними характеристиками системи і допускати кількісну оцінку на всіх етапах створення системи [13].

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, мети захисту інформації можуть бути досягнуті тільки шляхом створення системи захисту інформації (далі – СЗІ).

Система захисту інформації (СЗІ) - це складний комплекс програмних, технічних, криптографічних організаційних та інших засобів, методів і заходів, призначених для захисту інформації на основі комплексного підходу. Ефективність СЗІ можна охарактеризувати як здатність системи протистояти несанкціонованим діям порушника в рамках проектної загрози. Таким чином, ефективність СЗІ і характеризує рівень захищеності об'єкта.

Слід також пам’ятати що розробники засобів захисту інформації теж не стоять на місці. На кожну загрозу розробляється нове захисне програмне забезпечення або вдосконалюється вже наявне.

Таким чином основними інструментами забезпечення та підвищення ефективності захисту інформації є

- ідентифікація та аутентифікація;
- управління доступом;
- протоколювання і аудит;
- криптографічні методи.

2.3. Архітектура безпеки для систем, які забезпечують зв’язок між кінцевими пристроями

Архітектура захисту була створена для вирішення загальних питань захисту постачальників послуг, підприємств та споживачів та застосовується до бездротових, оптичних та провідних лініях зв'язку мереж передачі

мовлення, даних та інтегрованих мереж. Ця архітектура захисту визначає питання захисту для управління, контролю та використання мережевої інфраструктури, послуг та додатків. Архітектура захисту забезпечує комплексну, зверху вниз наскрізну область мережевого захисту і може застосовуватися до елементів мережі, послуг та додатків, щоб виявляти, прогнозувати та виправляти уразливість захисту.

Архітектура захисту логічно ділить складний набір наскрізних мережевих, пов'язаних з захистом параметрів, на окремі архітектурні компоненти. Такий поділ дозволяє застосовувати систематичний підхід до наскрізного захисту, який може використовуватися як для планування нових варіантів захисту, так і для оцінки захищеності існуючих мереж.

Архітектура захисту стосується трьох суттєвих питань наскрізного захисту:

1) Який захист необхідний і від яких загроз?

2) Які саме типи мережного обладнання та сукупності коштів повинні бути захищені?

3) Які саме типи мережної активності мають бути захищені?

Ці питання відносяться до трьох компонентів архітектури: вимірювання захисту, рівні захисту та площині захисту. Принципи, що задаються архітектурою захисту, можуть застосовуватися до широкого кола мереж незалежно від мережі або розташування в стеку протоколу.

У наступних розділах докладно описуються елементи архітектури та їх функції щодо головних загроз безпеці.

Рекомендація МСЭ-Т X.805 (10/2003)

Вимірювання захисту

Вимірювання захисту – це комплекс заходів захисту, призначених для реалізації конкретного аспекту мережного захисту. У цій Рекомендації ідентифікується вісім таких комплексів, що захищають від усіх основних загроз. Ці виміри не обмежені мережею, але також поширюються на

програми та інформацію кінцевого користувача. Крім того, вимірювання захисту застосовуються до постачальників послуг та організацій, що пропонує послуги із забезпечення безпеки своїм клієнтам. Вимірювання захисту [11]:

1) керування доступом;

2) автентифікація;

3) збереження інформації;

4) конфіденційність даних;

5) безпека зв'язку;

6) цілісність даних;

7) доступність;

8) таємність.

Вимірювання захисту: керування доступом

Вимірювання захисту – керування доступом – захищає від неправомірного використання мережевих ресурсів. Управління доступом гарантує, що лише уповноваженому персоналу або пристроям дозволено доступ до елементів мережі, збереженої інформації, потоків інформації, послуг та додатків. Крім того, управління доступом на основі ролей (RBAC) забезпечує різні рівні доступу для гарантії того, щоб люди і пристрої могли отримувати доступ і здійснювати операції тільки з тими елементами мережі, тією збереженою інформацією та з тими потоками інформації, доступ до яких їм дозволено.

Вимірювання захисту: автентифікація

Вимірювання захисту – автентифікація – призначене для посвідчення особи об'єктів, що підтримують зв'язок. Аутентифікація гарантує справжність особи об'єктів, що беруть участь у зв'язку (наприклад, людину, пристрої, послуги або програми), і забезпечує впевненість у тому, що об'єкт не намагається здійснювати заміну або неправомірно використовувати попередній сеанс зв'язку.

Вимірювання захисту: збереження інформації

Вимірювання захисту - збереження інформації - забезпечує засоби для запобігання з боку індивіда або об'єкта заперечення виконання конкретної дії, пов'язаного з даними, забезпечуючи наявність доказів здійснення різних дій, пов'язаних із мережею (таких як доказ зобов'язання, наміри або готовності;доказ походження даних, доказ власності, доказ використання ресурсу). Гарантується наявність даних, які можуть бути надані третій стороні і які можуть використовуватися як докази того, що деяка подія чи дія мала місце.

Вимірювання захисту: конфіденційність даних

Вимірювання захисту – конфіденційність даних – захищає дані від неправомірного розкриття. Конфіденційність даних гарантує, що зміст даних не може бути зрозуміло об'єктами, які мають цього права. Шифрування, списки контролю доступу та дозвіл доступу до файлів – це методи, які часто використовуються для забезпечення конфіденційності даних.

Вимірювання захисту: безпека зв'язку

Вимірювання захисту – безпека зв'язку – гарантує, що інформація передається лише між уповноваженими кінцевими точками (інформація не змінює напряму та не перехоплюється під час передачі між цими кінцевими точками).

Вимірювання захисту: цілісність даних

Вимірювання захисту – цілісність даних – гарантує правильність та точність даних. Дані захищені від несанкціонованої зміни, видалення, створення та дублювання, а також забезпечується виявлення такої несанкціонованої діяльності.

Вимірювання захисту: доступність

Напрямок захисту – доступність – гарантує відсутність будь-якого обмеження на санкціонований доступ до елементів мережі, інформації, що

зберігається, потоків даних, до послуг та програм через події, що впливають на мережу. Варіанти відновлення після аварій включені до цієї категорії.

Вимірювання захисту: секретність

Вимірювання захисту – секретність – забезпечує захист інформації, яка б могла бути отримана, виходячи із спостереження мережевої діяльності. Приклади такої інформації Web-сайти, які користувач відвідав, географічне розташування користувача, IP-адреси та імена DNS у мережі постачальника послуг.

Рівні захисту

Для забезпечення наскрізного захисту вимірювання захисту, описані вище, повинні застосовуватися до ієрархії мережного обладнання та груп коштів, що визначаються як рівні захисту. У цій Рекомендації визначаються три рівні захисту [11]:

– рівень захисту інфраструктури;

– рівень захисту послуг; і

– рівень захисту програм.

Ці рівні у комплексі забезпечують мережеві рішення.

Рівні захисту – це низка факторів, що сприяють забезпеченню мережевого захисту: рівень інфраструктури уможливлює застосування рівня послуг, а рівень послуг робить можливе застосування рівня додатків. Архітектура захисту враховує той факт, що кожен рівень має різні точки вразливості захисту, і пропонує гнучкість у відображення потенційних загроз найбільш прийнятним способом для конкретного рівня захисту.

Необхідно зазначити, що рівні захисту (як визначено вище) представляють окрему категорію, і всі три рівні захисту можуть застосовуватися до кожного рівня еталонної моделі ВОС. Рівні захисту визначають, де захист має бути використаний у програмах та рішеннях, забезпечуючи послідовну структуру мережного захисту. Наприклад, спочатку вразливість захисту розглядається на рівні інфраструктури, потім на

рівні послуг та, нарешті, вразливість захисту розглядається лише на рівні додатків. На малюнку 1 показано як вимірювання захисту застосовуються до рівнів захисту для зменшення вразливості, яка існує на кожному рівні, і таким чином пом'якшують наслідки атак на захист.

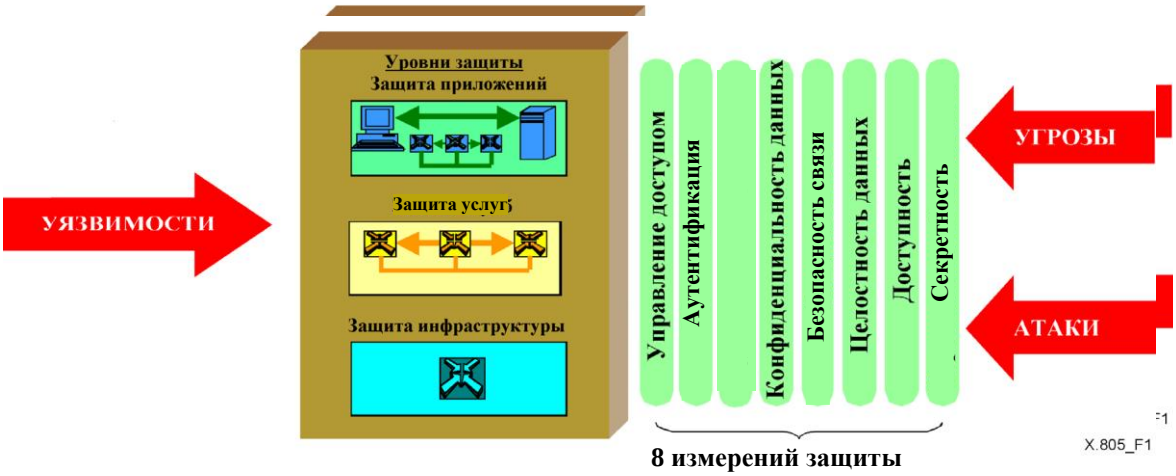

Рис. 2.1 Застосування вимірювань захисту до рівнів захисту

Рівень захисту інфраструктури.

Рівень захисту інфраструктури складається з мережевих засобів передачі, а також окремих елементів мережі, захищених за вимірами захисту. Рівень інфраструктури включає основні стандартні блоки мереж, їх послуги та програми. Прикладами компонентів, що належать до рівня інфраструктури, можуть бути окремі маршрутизатори, комутатори та сервери, а також лінії зв'язку між окремими маршрутизаторами, комутаторами та серверами.

Рівень захисту послуг.

Рівень захисту послуг визначає захист послуг, які постачальники послуг надають своїм клієнтам. До таких послуг відносяться як базові транспорт та підключення до необхідних для обслуговування ресурсів, наприклад, необхідних для забезпечення доступу до Інтернету (служби AAA, служби динамічної конфігурації хостів, служби імен доменів і т. д.), так і

додаткові послуги, такі як послуги безкоштовної телефонії, QoS, VPN, служби позиціонування, миттєвої передачі повідомлень тощо. Рівень захисту послуг використовується для захисту постачальників послуг та їх клієнтів, які є потенційними об'єктами загроз захисту. Наприклад, нападники можуть намагатися позбавити постачальника послуг можливості надавати послуги або перервати обслуговування окремого клієнта постачальника послуг (наприклад, корпорації).

Рівень захисту програм.

На рівні захисту програм забезпечується головним чином захист мережевих програм, до яких мають доступ клієнти постачальника послуг. Робота таких програм забезпечується мережевими службами і включає основний транспорт файлів (наприклад, FTP) і програми навігації в мережі, основні програми, такі як робота з директоріями, мережна передача мовних повідомлень та електронна пошта, а також більш складні програми, такі як управління взаємодією з клієнтами, електронна торгівля/торгівля за допомогою рухомого зв'язку, професійна підготовка на основі мережі, відеоконференції і т. д. власних (чи орендованих) центрах даних. На цьому рівні є чотири потенційні об'єкти нападу: користувач додатків, постачальник програм, що зв'язує програмне забезпечення, надане сторонніми інтеграторами (наприклад, службами хостингу мережі), та постачальник послуг.

Площини захисту.

Площина захисту – це певний тип мережевої операції, захищеної вимірами захисту. У цій Рекомендації визначається три площини захисту для представлення трьох типів захищених мережевих операцій. Визначаються такі площини захисту [11]:

1) площину керування;

2) площину контролю;

3) площину кінцевого користувача.

Ці площини захисту відносяться до конкретних потреб у захисті, пов'язаних з керуванням мережею, контролем за мережею або сигнальними операціями, а також операціями кінцевого користувача відповідно.

Мережі слід проектувати таким чином, щоб події в одній площині захисту були повністю ізольовані з інших площин захисту. Наприклад, приплив пошуків DNS у площині кінцевого користувача, ініційований запитами кінцевого користувача, не повинен блокувати інтерфейс OAM&P у площині управління, який дозволить адміністратору вирішити цю проблему.

На рисунку 2.2 показана архітектура захисту, що включає площини захисту. Кожен тип описаних мережевих операцій має власні конкретні потреби у сфері захисту. Концепція площин захисту дозволяє диференціювати конкретні проблеми захисту, пов'язані з цими операціями, і дозволяє вирішувати їх незалежно. Розглянемо, наприклад, службу VoIP, до якої належить рівень захисту послуг. Захист управління службою VoIP (наприклад, підключення користувачів) не повинен залежати від захисту контролю за послугами (наприклад, протоколів типу SIP), а також не повинен залежати від захисту даних кінцевого користувача, що передаються службою (наприклад, мова користувача).

Площина захисту управління

До площини захисту управління належить захист функцій OAM&P е[illegible]

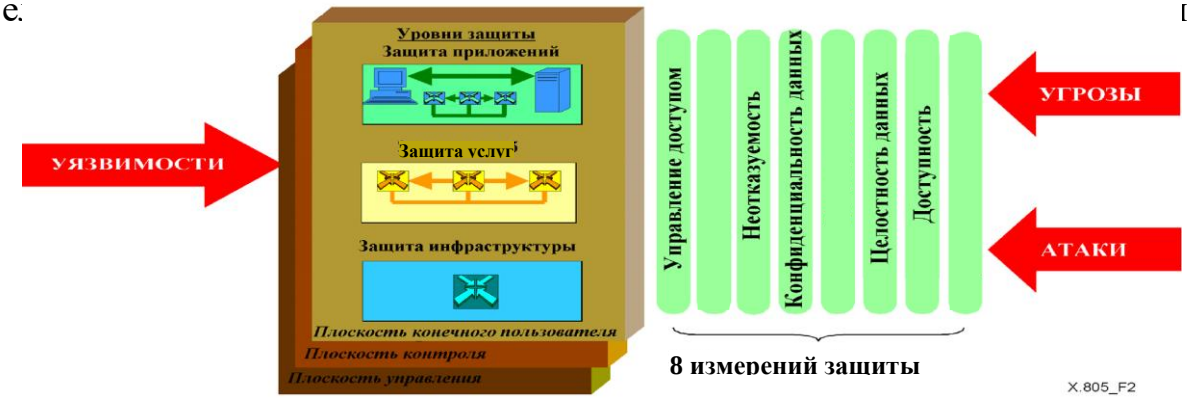

Рис. 2.2 Площини захисту показують різні типи мережевих операцій.

виконання операцій, системи підтримки ділових операцій, системи роботи з клієнтом тощо), а також центри даних. Площина управління підтримує функції роботи з помилками, забезпечення продуктивності, управління, забезпечення та захисту (FCAPS). Слід зазначити, що мережа, по якій здійснюється трафік для цих операцій, може перебувати в смузі або поза смужою трафіку користувача постачальника послуг.

Площина захисту контролю

До площини захисту контролю належить захист операцій, які забезпечують ефективну доставку інформації, послуг та додатків через мережу. Зазвичай використовується передача інформації з одного пристрою на інший, що дозволяє пристрої (наприклад, комутаторів або маршрутизаторів) визначати оптимальний спосіб направлення або перемикання трафіку через базову транспортну мережу. Цей тип інформації іноді називається керуючою або сигнальною інформацією. Мережа, яка надсилає такі типи повідомлень, може знаходитися в смузі або поза смужою трафіку користувача постачальника послуг. Наприклад, IP-мережі передають таку керуючу інформацію у смузі, тоді як КТСОП передає свою керуючу інформацію окремої позасмугової сигнальної мережі (мережі SS7). Приклади такого типу трафіку включають протоколи маршрутизації, DNS, SIP, SS7, Megaco/H.248 і т. д.

Площина захисту кінцевого користувача

До площини захисту кінцевого користувача відноситься захист доступу клієнтів до мережі постачальника послуг та її використання. До цієї площини відносяться реальні потоки даних кінцевого користувача. Кінцеві користувачі можуть використовувати мережу, яка тільки забезпечує зв'язок, і вони також можуть використовувати її для служб додаткових послуг, таких як VPN, або вони можуть використовувати цю мережу для доступу до мережних програм.

Загрози безпеки

Архітектура захисту визначає план і низку принципів, які описують структуру захисту варіанта наскрізного захисту. Архітектура визначає, які проблеми захисту мають бути вирішені для запобігання навмисним загрозам, а також випадковим загрозам. Наступні загрози описані в Рекомендації МСЕ-Т X.800 (1991), Архітектура захисту для взаємозв'язку відкритих систем для застосування МККТТ:

• знищення інформації та/або інших ресурсів;

• спотворення чи зміна інформації;

• крадіжка, видалення чи втрата інформації та/або інших ресурсів;

•розкриття інформації;

• переривання обслуговування.

Перетин кожного рівня захисту з кожною площиною захисту являє собою область захисту, в якій вимірювання захисту застосовуються для протидії загрозам. У таблиці 2.1 представлено схематичне співвідношення вимірювань захисту стосовно загроз безпеки. Співвідношення ідентичне кожної області захисту.

'Так в осередку, сформованому перетином стовпців та рядків таблиці, означає, що конкретній загрозі безпеці протистоїть відповідний вимір захисту.

На рисунку 2.3 показано архітектуру захисту з елементами архітектури та вказівкою загроз безпеки, описаних вище. На рисунку представлена концепція захисту мережі за вимірами захисту у кожній площині захисту кожного рівня захисту, щоб представити комплексний варіант захисту. Слід зазначити, що залежно від потреб захисту цієї мережі не обов'язково реалізовувати всі елементи архітектури (тобто мати повну систему вимірювань захисту, рівнів захисту та площин захисту).

Таблиця 2.1.
Співвідношення вимірювань захисту та загроз безпеки

Вимірювання захисту	Загроза безпеки				
	Знищення інформації або інших ресурсів	Спотворення або зміна інформації	Крадіжка, видалення або втрата інформації та інших ресурсів	Розкриття інформації	Переривання обслуговування
Управління доступом	ТАК	ТАК	ТАК	ТАК	
Аутентифікациія			ТАК	ТАК	
Збереженість інформації	ТАК	ТАК	ТАК	ТАК	ТАК
Конфіденціальність даних			ТАК	ТАК	
Безпека зв'язку			ТАК	ТАК	
Цілісність даних	ТАК	ТАК			
Доступність	ТАК				ТАК
Секретність				ТАК	

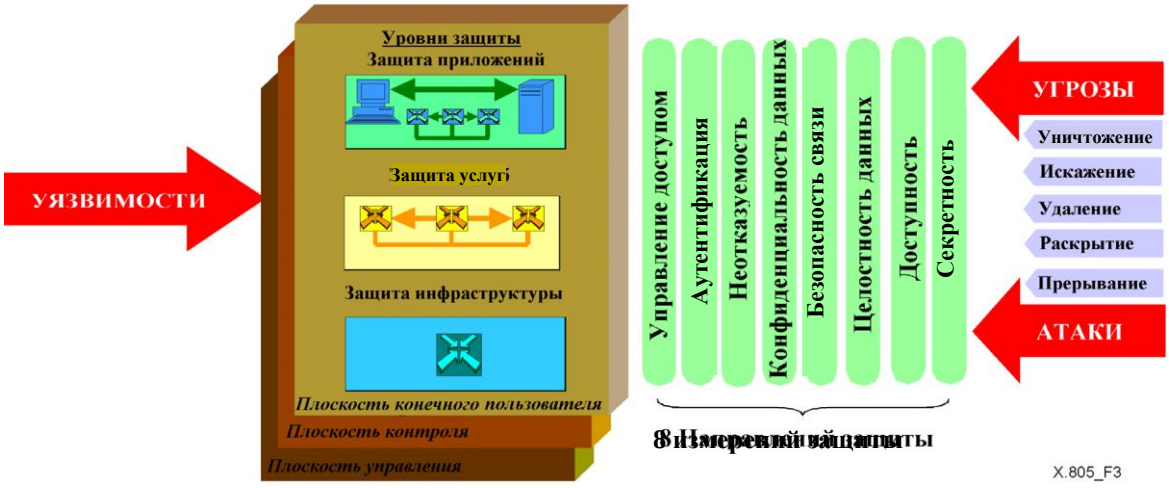

Рис. 2.3. Архітектура захисту для сквозного мережевого захисту

Опис цілей, що досягаються застосуванням вимірювань захисту до рівня захисту.

Архітектура захисту може застосовуватися до всіх аспектів та фаз програми захисту, як показано на рис. 2.4. Як випливає з рис. 2.4, програма захисту складається зі стратегій та процедур на додаток до технології та проходить через три фази протягом терміну своєї дії:

1) фаза визначення та планування;

2) фаза реалізації;

3) фаза експлуатації.

Архітектура захисту може застосовуватися до стратегій та процедур захисту, а також технології протягом усіх трьох фаз програми захисту.

Архітектура захисту може визначати розробку комплексних визначень політики захисту, реакції на події та планів відновлення, а також архітектури технології, беручи до уваги кожен вимір захисту на кожному рівні та в кожній площині захисту у фазі визначення та планування. Архітектура захисту може також використовуватися як основа для оцінки захисту, в ході якої досліджувалося б, як виконання програми захисту співвідноситься з вимірюваннями, рівнями та площинами захисту, у міру того, як розробляються стратегії та процедури та реалізується технологія. Коли програма захисту розгорнута, вона повинна підтримуватися для збереження адекватності в середовищі, що постійно змінюється. Архітектура захисту може допомагати в управлінні стратегіями та процедурами захисту, реакцією на події та реалізацією планів відновлення, а також в управлінні архітектурою технології, гарантуючи, що модифікації програми захисту застосовуються до кожного вимірювання захисту на кожному рівні та в кожній площині захисту.

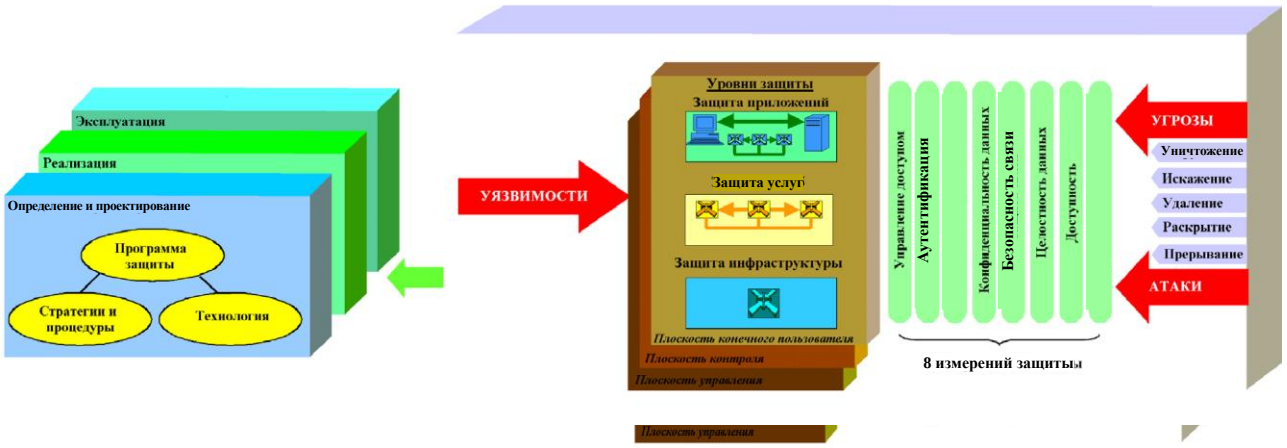

Рис. 2.4 Застосування архітектури захисту до програм захисту

Крім того, архітектура захисту може застосовуватися до будь-якого типу мережі будь-якого рівня стека протоколу. Наприклад, в IP-мережі, що знаходиться на третьому рівні стека протоколу, до рівня інфраструктури відносяться окремі маршрутизатори, прямі канали зв'язку між маршрутизаторами (наприклад, SONET, ATM PVC тощо) та серверні платформи, що використовуються для забезпечення допоміжних послуг, необхідні IP-мережі [12]. До рівня послуг відноситься безпосередньо основна послуга IP (наприклад, можливість підключення до Інтернету), допоміжні послуги IP (наприклад, AAA, DNS, DHCP тощо) та розширені додаткові послуги, що пропонуються постачальником послуг (наприклад, VoIP, QoS, VPN і т.д.). Нарешті, до рівня програм відноситься захист програм користувача, доступ до яких забезпечується по IP-мережі (наприклад, електронна пошта тощо).

Аналогічно, для мережі ATM, яка знаходиться на другому рівні стека протоколу, до рівня інфраструктури відносяться окремі комутатори та прямі канали зв'язку між комутаторами (засоби передачі, наприклад DS-3). До рівня послуг відносяться різні класи транспорту, що забезпечується запропонованою службою ATM (постійна швидкість передачі, змінна швидкість передачі в

режимі реального часу, змінна швидкість передачі інформації не в режимі реального часу, наявна швидкість передачі та швидкість передачі). Нарешті, до рівня програм відносяться програми, для доступу до яких кінцевий користувач використовує мережу АТМ, наприклад, програму відеоконференцзв'язку.

На рис. 2.5 представлена схема архітектури захисту в табличній формі та показаний методичний підхід до забезпечення захисту мережі. Як можна бачити на малюнку, перетин рівня захисту з площиною захисту представляє єдину перспективу для розгляду восьми вимірювань захисту. Кожен із цих дев'яти модулів поєднує вісім вимірювань захисту, які застосовуються до конкретного рівня захисту у певній площині захисту. Слід зазначити, що вимірювання захисту різних модулів мають різні цілі та, отже, включають різні комплекси заходів захисту. Таблична форма є зручним способом опису цілей вимірювань захисту для кожного модуля.

Захист рівня інфраструктури

Захист площини управління рівня інфраструктури передбачає захист експлуатації, управління, технічного обслуговування та забезпечення (OAM&P) окремих елементів мережі, ліній зв'язку та серверних платформ, у тому числі складається мережу. Конфігурація мережевих пристроїв та ліній зв'язку також вважається операцією управління. Приклад керування інфраструктурою, який має бути захищений, – це конфігурація окремого маршрутизатора або комутатора персоналом, який відповідає за мережеві операції. У таблиці 2.2 описані цілі застосування вимірювань захисту рівня інфраструктури в площині управління.

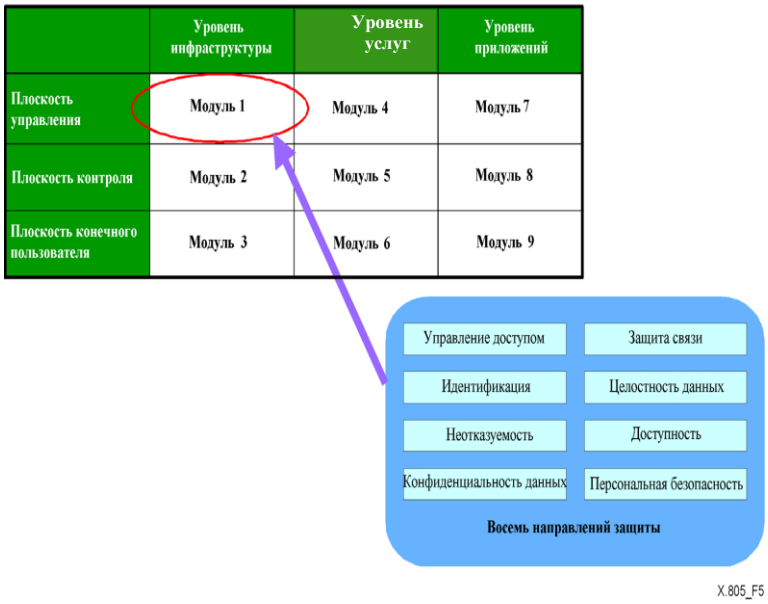

Рис. 2.5 Архітектура захисту у табличній формі

Захист у площині управління рівня інфраструктури полягає у захисті управлінської або сигнальної інформації, яка знаходиться в елементах мережі та серверних платформах, з яких складається мережа, а також у захисті отримання та передачі управлінської чи сигнальної інформації мережею, елементами та серверними платформами. Наприклад, таблиці комутації, що у мережних комутаторах, повинні бути захищені від втручання чи неправомочного розкриття. Ще в одному прикладі маршрутизатори повинні бути захищені від прийому та розповсюдження фальшивих модифікацій маршрутизації та реакції на фальшиві запити маршрутизації, що походять від фіктивних маршрутизаторів. У таблиці 2.3 описані цілі застосування вимірювань захисту рівня інфраструктури в площині контролю.

Таблиця 2.2.

Застосування вимірювань захисту до рівня інфраструктури у площині управління

Модуль 1: Рівень інфраструктури, площина управління	
Вимірювання захисту	**Мети захисту**
Управління доступом	Гарантувати, що лише уповноваженому персоналу або пристроям (наприклад, у разі SNMP – керованим пристроям) дозволено виконувати адміністративні дії чи операції керування на мережевому пристрої чи лінії зв'язку. Це стосується як прямого управління пристроєм через консольний порт, так і дистанційного управління пристроєм.
Аутентифікація	Перевірити особистість людини або пристрою, який виконує адміністративні дії або операції управління на мережному пристрої або лінії зв'язку. Як елемент керування доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує людину або пристрій, що виконують кожну адміністративну дію або операцію управління на мережевому пристрої або лінії зв'язку, та дію, яка була виконана. Цей звіт може використовуватись як підтвердження джерела адміністративних чи управлінських дій.
Конфіденційність даних	Захищати інформацію про конфігурацію мережного пристрою або лінії зв'язку від несанкціонованого доступу та перегляду. Це застосовується до інформації про конфігурацію, яка є в мережному пристрої або лінії зв'язку, до інформації про конфігурацію, що передається на мережевий пристрій або лінію зв'язку, а також до резервної інформації про конфігурацію, що зберігається автономно. Захистити адміністративну інформацію про аутентифікацію (наприклад, ідентифікацію адміністратора та паролі) від несанкціонованого доступу та перегляду. Методи, що використовуються для управління доступом, можуть сприяти конфіденційності даних.
Безпека зв'язку	У разі дистанційного керування мережевим пристроєм або лінією зв'язку гарантувати, що управлінська інформація передається лише між станціями дистанційного керування та пристроями або лініями зв'язку, керування якими здійснюється. Управлінська інформація не змінює напрями і перехоплюється під час передачі між цими кінцевими точками. Такі ж заходи вживаються стосовно адміністративної інформації про аутентифікацію (наприклад, ідентифікація адміністратора та паролі).
Цілісність даних	Захищати інформацію про конфігурацію мережевих пристроїв та ліній зв'язку від несанкціонованої модифікації, видалення, створення та дублювання. Цей захист застосовується до інформації про конфігурацію, що міститься в мережному пристрої або лінії зв'язку, а також до інформації про конфігурацію, яка передається транзитом або зберігається автономно. акі ж заходи вживаються стосовно адміністративної інформації про аутентифікацію (наприклад, ідентифікація адміністратора та паролі).
Доступність	Гарантувати, що уповноваженому персоналу або пристроям не може бути відмовлено у здатності керувати мережевим пристроєм або лінією зв'язку. Це включає захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення адміністративної інформації щодо ідентифікації (наприклад, ідентифікація адміністратора та паролів).
Секретность	Гарантировать, что информация, которая может использоваться для идентификации сетевого устройства или линии связи, не доступна неуполномоченным персоналу или устройствам. Примеры такого типа информации включают IP-адрес сетевого устройства и имя домена DNS. Например, способность идентифицировать сетевое устройство дает целевую информацию атакующим.

Таблиця 2.3.
Застосування вимірювань захисту до рівня інфраструктури у площині контролю

Модуль 2: Рівень інфраструктури, плщина контролю	
Вимсірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженому персоналу та пристроям дозволено доступ до інформації про керування доступом, що знаходиться у мережному пристрої (наприклад, таблиці маршрутизації) або в автономній пам'яті. Гарантувати, що мережевий пристрій приймає повідомлення про керування лише від уповноважених мережних пристроїв (наприклад, коригування маршруту).
Аутентифікація	Перевірити особистість людини або пристрою, який читає або змінює інформацію про керування, що знаходиться в мережевому пристрої. Перевірити особистість пристрою, який надсилає інформацію про керування мережним пристроєм. Як елемент управління доступом можуть знадобитися методи аутентифікації.
Збереженість інформації	Формувати звіт, який ідентифікує людину або пристрій, які читали або змінили інформацію про управління в мережевому пристрої або лінії зв'язку, а також дію, яка була ними виконана. Цей звіт може використовуватись як підтвердження доступу до інформації про управління або її зміни. Формувати звіт, що ідентифікує пристрій, від якого виходять повідомлення про керування, що надсилаються мережному пристрою, а також дію, яка була виконана. Цей звіт може використовуватися як доказ того, що пристрій став джерелом повідомлення про керування.
Конфіденційність даних	Захищати інформацію про керування, що знаходиться в мережному пристрої або автономній пам'яті, від несанкціонованого доступу та перегляду. Методи, що використовуються для керування доступом, можуть сприяти конфіденційності інформації про управління, що знаходиться в мережному пристрої. Захищати інформацію про керування, призначену для мережного пристрою, від несанкціонованого доступу та перегляду під час передачі через мережу.
Безпека зв'язку	Гарантувати, що інформація про управління, що передається по мережі (наприклад, коригування маршруту), передається лише від джерела інформації про управління до бажаного адресата. Інформація про управління не змінює напрями і не перехоплюється в ході передачі між цими точками.
Цілісність даних	Захищати інформацію про керування, що знаходиться в мережевих пристроях і передається по мережі або зберігається автономно, від несанкціонованої модифікації, видалення, створення та дублювання.
Доступність	Гарантуйте, що мережні пристрої завжди доступні для отримання інформації про керування з уповноважених джерел. Це включає захист від навмисних нападів, таких як відмова в обслуговуванні (DoS), а також від випадкових випадків (наприклад, спотворення маршруту).
Секретність	Гарантувати, що інформація, яка може використовуватися для ідентифікації мережного пристрою або лінії зв'язку, не доступна для неуповноважених персоналу або пристроїв. Приклади такого типу інформації включають IP-адресу мережного пристрою та ім'я домену DNS. Наприклад, здатність ідентифікувати мережеві пристрої чи лінії зв'язку дає атакуючим цільову інформацію.

Захист площини кінцевого користувача рівня інфраструктури полягає у захисті інформації та мовних сигналів користувача, якщо вони знаходяться в елементах мережі або передаються через них, а також коли вони передаються лініями зв'язку. Сюди також

відноситься захист інформації користувача, що знаходиться на серверній платформі, а також захист інформації користувача від незаконного перехоплення під час передачі елементами

Таблиця 2.4.
Застосування вимірювань захисту до рівня інфраструктури у площині кінцевого користувача

Модуль 3: Рівень інфраструктури, площина кінцевого користувача	
Вимірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженому персоналу або пристроям дозволено доступ до даних кінцевого користувача, що передаються по елементу мережі або лінії зв'язку або знаходяться в автономних пристроях пам'яті.
Аутентифіка-ція	Перевірити особистість людини або пристрою, який прагне отримати доступ до даних кінцевого користувача, які передаються по елементу мережі або лінії зв'язку або знаходяться в автономних пристроях пам'яті. Як елемент керування доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує кожну людину або пристрій, які отримують доступ до даних кінцевого користувача, що передаються по елементу мережі або лінії зв'язку або знаходяться в автономних пристроях пам'яті, та дію, яка була виконана. Цей звіт повинен використовуватись як підтвердження доступу до даних кінцевого користувача.
Конфіденційність даних	Захищати дані кінцевого користувача, які передаються по елементу мережі або лінії зв'язку або знаходяться в автономних пристроях пам'яті, від несанкціонованого доступу та перегляду. Методи, що використовуються для керування доступом, можуть сприяти конфіденційності даних кінцевого користувача.
Безпека зв'язку	Гарантувати, що дані кінцевого користувача, які передаються по елементу мережі або лінії зв'язку, не змінюють напрями і не перехоплюються без санкціонованого доступу (наприклад, законний перехоплення), коли між кінцевими точками.
Цілісністьданих	Захищати дані кінцевого користувача, які передаються елементом мережі або лінії зв'язку або знаходяться в автономних пристроях, від несанкціонованої модифікації, видалення, створення або дублювання.
Доступність	Гарантувати, що уповноважений персонал (включаючи кінцевого користувача) та пристрої не можуть бути позбавлені доступу до даних кінцевого користувача в автономних пристроях. Сюди належить захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення інформації про аутентифікацію (наприклад, ідентифікація користувача та його паролі, ідентифікація адміністратора та його паролі).
Секретність	Гарантувати, що елементи мережі не надають інформації, що стосується мережі кінцевого користувача (наприклад, географічне розташування користувача, відвідувані Web-сайти тощо), неуповноваженому персоналу або пристроям.

мережі або лініями зв'язку. У таблиці 2.4 описані цілі застосування вимірювань захисту рівня інфраструктури в площині кінцевого користувача.

Захист рівня послуг

Захист рівня послуг ускладнюється тим, що послуги можуть взаємно посилюватися задоволення вимог клієнта. Наприклад, щоб забезпечити послугу VoIP, постачальник послуг

повинен спочатку забезпечити базову послугу IP з її необхідними допоміжними послугами, такими як AAA, DHCP, DNS і т. д. та безпеки для послуги VoIP. Тому аналізована пропонована послуга має бути розбита на складові послуги для забезпечення захисту загалом.

Захист площини управління рівнями послуг полягає в захисті функцій OAM&P мережевих служб. Конфігурація мережевих послуг вважається операцією управління. Прикладом захисту управління послугами, що вимагає захисту, є забезпечення уповноважених користувачів IP-послуги персоналом, що займається експлуатацією мереж. У таблиці 2.5 описані цілі застосування вимірювань захисту рівня послуг у площині управління.

Таблиця 2.5.
Застосування вимірювань захисту до рівня послуг у площині управління

Модуль 4: Рівень служб, площина управління	
Вимірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженому персоналу та пристроям дозволено виконувати адміністративні дії та операції управління мережевою послугою (наприклад, забезпечувати користувачів послуги).
Аутентифікація	Перевірити особу людини або пристрою, що прагне виконати адміністративні дії або операції керування мережевою послугою. Як частина управління доступом можуть знадобитися методи автентифікації
Збереженість інформації	Формувати звіт, що ідентифікує людину або пристрій, що виконують кожну адміністративну або управлінську дію мережевої послуги, та дії, що були виконані. Цей звіт повинен використовуватися як підтвердження того, що зазначена особа або пристрій виконали адміністративні чи управлінські операції.
Конфиденциальность данных	Захищати інформацію про конфігурацію мереж послуги та управлінську інформацію (наприклад, завантажені IPSec параметри налаштування клієнта для послуги VPN) від несанкціонованого доступу та перегляду. Це застосовується до інформації про управління та конфігурації, що знаходиться в мережевих пристроях і передається по мережі або зберігається автономно. Захищати адміністративну та управлінську інформацію мережевої послуги (наприклад, ідентифікацію користувача та його паролі, ідентифікацію адміністратора та його паролі) від несанкціонованого доступу та перегляду.
Безпека зв'язку	У разі дистанційного керування мережевою послугою гарантувати, що адміністративна та управлінська інформація передається лише від дистанційної станції керування до пристроїв, керування якими провадиться в рамках мережевої послуги. Адміністративна та управлінська інформація не змінює напрями та не перехоплюється при передачі між цими кінцевими точками. Такі ж заходи вживаються щодо інформації про аутентифікацію мережевої послуги (наприклад, ідентифікація користувача та його паролі, ідентифікація адміністратора та його паролі).
Цілісність даних	Захищати адміністративну та управлінську інформацію мережевих послуг від несанкціонованої модифікації, видалення, створення чи дублювання. Цей захист застосовується до адміністративної та управлінської інформації, що знаходиться в мережевих пристроях і передається по мережі або зберігається в автономних системах. Такі ж заходи вживаються щодо інформації про аутентифікацію мережевої послуги (наприклад, ідентифікація користувача та його паролі, ідентифікація адміністратора та його паролі).

Продовження таблиці 2.5

Доступність	Гарантувати, що уповноважений персонал та пристрої не можуть бути позбавлені можливості керувати мережевою послугою. Сюди належить захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення адміністративної інформації про автентифікацію мережі (наприклад, ідентифікація адміністратора та його паролі).
Секретність	Гарантувати, що інформація, яка може використовуватися для ідентифікації адміністративної та управлінської систем мережі, не доступна неуповноваженому персоналу або пристроям. Приклади такого типу інформації включають IP-адресу системи та ім'я домену DNS. Наприклад, здатність ідентифікувати адміністративні системи мережевої послуги дає атакуючим цільову інформацію.

Захист площини контролю рівня послуг полягає у захисті інформації про керування або сигнальну інформацію, використовувану мережевою послугою. Наприклад, сюди належать проблеми захисту протоколу SIP, який використовується, щоб ініціювати та підтримувати сеанси VoIP. У таблиці 2.6 описані цілі застосування вимірювань захисту рівня послуг у площині контролю.

Таблиця 2.6.

Застосування вимірювань захисту до рівня послуг у площині кінцевого користувача

Модуль 5: Рівень послуг, площина кінцевого користувача	
Вимірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженим користувачам та пристроям забезпечено доступ до мережі та її використання..
Аутентифіка-ція	Перевірити особистість користувача або пристрою, який прагне отримати доступ до мережі та її використовувати. Як елемент управління доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує кожного користувача та пристрій, які отримали доступ до мережі та використовували її, а також дію, яка була при цьому виконана. Цей звіт повинен використовуватися як підтвердження доступу до мережі та її використання кінцевим користувачем або пристроєм.
Конфиденційність даних	Захищати дані кінцевого користувача, які передаються, обробляються або зберігаються мережевою послугою, від несанкціонованого доступу та перегляду. Методи, що використовуються для керування доступом, можуть сприяти конфіденційності даних.
Безпека зв'язку	Гарантувати, що дані кінцевого користувача, які передаються, обробляються або зберігаються мережевою послугою, не змінюють напрями та не перехоплюються без санкціонованого доступу (наприклад, законне перехоплення), під час передачі між цими кінцевими точками.
Цілісність даних	Захищати дані кінцевого користувача, які передаються, обробляються або зберігаються мережевою послугою від несанкціонованої модифікації, видалення, створення або дублювання.
Доступність	Гарантувати, що уповноваженим кінцевим користувачам та пристроям не може бути відмовлено у доступі до мережі. Сюди належить захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення інформації про аутентифікацію кінцевого користувача (наприклад, ідентифікація користувача та паролі).
Секретність	Гарантувати, що мережна послуга не надає інформацію, що стосується використання кінцевим користувачем (наприклад, для VoIP – сторони, що викликаються), неуповноваженому персоналу або пристроям.

Захист рівня додатків.

Таблиця 2.7.

Застосування вимірювань захисту до рівня додатків у площині управління

Модуль 6: Рівень додатка, площина управління	
Вимірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженому персоналу та пристроям дозволяється виконувати адміністративні дії та операції керування мережевою програмою (наприклад, керувати поштовими скриньками користувачів для програми електронної пошти).
Аутентифіка-ція	Перевіряти особу людини або пристрою, що прагне здійснювати адміністративні дії або операції керування мережевим додатком. Як частина управління доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує людину або пристрій, які виконують кожну адміністративну дію або операцію з управління мережним додатком, а також дію, яка була виконана. Цей звіт повинен використовуватися як підтвердження того, що адміністративна дія або операція управління було виконано, із зазначенням людини або пристрою, які це вчинили.
Конфиденційність даних	Захищати всі файли, які використовуються при створенні та виконанні мережевої програми (наприклад, вихідні файли, об'єктні файли, файли, тимчасові файли тощо), а також файли конфігурації програми від несанкціонованого доступу та перегляду. Це стосується файлів програм, що знаходяться в мережевих пристроях і які передаються по мережі або зберігаються автономно. Захищати адміністративну та управлінську інформацію мережі (наприклад, ідентифікацію користувача та його паролі, ідентифікацію адміністратора та його паролі) від несанкціонованого доступу та перегляду.
Безпека зв'язку	У разі дистанційного керування мережевим додатком гарантувати, що адміністративна та управлінська інформація передається тільки від дистанційної віддаленої станції керування до пристроїв, що становлять мережевий додаток. Адміністративна та управлінська інформація не змінює напрями та не перехоплюється при передачі між цими кінцевими точками. Ті ж заходи вживаються стосовно адміністративної та управлінської інформації мережевого додатка (наприклад, ідентифікація користувача та його паролі, ідентифікація адміністратора та його паролі).
Цілісність даних	Захищати всі файли, що використовуються при створенні та виконанні мережевої програми (наприклад, вихідні файли, об'єктні файли, файли, тимчасові файли і т. д.), а також файли конфігурації програми від несанкціонованої модифікації, видалення, створення або дублювання. Цей захист також забезпечується файлами, що знаходяться в мережевих пристроях і передаються по мережі або зберігаються автономно. Ті ж заходи застосовуються до адміністративної та управлінської інформації мережевого додатка (наприклад, ідентифікація користувача та його паролі, ідентифікація адміністратора та його паролі).
Доступність	Гарантувати, що уповноваженому персоналу та пристроям не може бути відмовлено у здатності керувати мережевим додатком. Сюди належить захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення адміністративної інформації про автентифікацію мережевої програми (наприклад, ідентифікація адміністратора та його паролі).
Секретність	Гарантувати, що інформація, яка може бути використана для ідентифікації адміністративних або управлінських систем мережного додатка, не доступна неуповноваженому персоналу та пристроям. Приклади такого типу інформації включають IP-адресу мережного пристрою та ім'я домену DNS. Наприклад, здатність ідентифікувати адміністративні системи мережного додатка дає атакуючим цільову інформацію.

Захист площини управління рівня програм полягає у захисті функцій OAM&P мережного додатка. Конфігурація мережевих додатків також вважається операцією управління. площині управління.

Захист площини контролю рівня додатків полягає у захисті контрольної або сигнальної інформації, що використовується мережними програмами. Цей тип інформації зазвичай спонукає програму виконувати дію у відповідь прийом інформації. Наприклад, тут розглядаються проблеми захисту протоколів SMTP та POP, які використовуються для керування доставкою електронної пошти. У таблиці 2.8 описуються цілі застосування вимірювань захисту рівня додатків у площині контролю.

Таблиці 2.8.

Застосування вимірювань захисту до рівня додатків у площині контролю

Модуль 7 Рівень додатків, площина контролю	
Вимірювання захисту	**Цели защиты**
Управління доступом	Гарантувати до прийняття повідомлення, що інформація про керування програмою, отримана мережевим пристроєм, що бере участь у мережному додатку, походить з уповноваженого джерела (наприклад, повідомлення SMTP, що запитує передачу електронної пошти). Наприклад, захист від спуфінгу з боку неуповноваженого пристрою клієнта SMTP.
Аутентифіка-ція	Перевірити походження інформації про керування програмою, яка надсилається мережевим пристроям, що беруть участь у мережному додатку. Як частина управління доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує людину або пристрій, що є джерелом повідомлень про керування додатком, одержуваним мережевим пристроєм, що бере участь у мережному додатку, а також дію, яка була виконана. Цей звіт може використовуватися як підтвердження того, що людина або пристрій стали джерелом повідомлення про керування програмою.
Конфиденциій ність даних	Захищати інформацію про керування програмою, що знаходиться в мережному пристрої (наприклад, бази даних про сеанси SSL) і передається по мережі або зберігається автономно, від несанкціонованого доступу та перегляду. Методи, що використовуються для керування доступом, можуть сприяти конфіденційності даних про керування мережевою програмою, що знаходяться в мережному пристрої.
Безпека зв'язку	Гарантувати, що інформація про керування програмою, що передається по мережі (наприклад, повідомлення про погодження SSL), передається лише від джерела інформації про керування до бажаного адресата. Інформація про управління додатком не змінює напрями і не перехоплюється під час передачі між цими кінцевими точками.
Цілісність даних	Захищати інформацію про керування мережевим додатком, що знаходиться в мережевих пристроях і передається по мережі або зберігається автономно, від несанкціонованої модифікації, видалення, створення або дублювання.

Продовження таблиці 2.8

Доступність	Гарантувати, що мережні пристрої, що беруть участь у мережних програмах, завжди доступні для отримання інформації про управління з уповноважених джерел. Сюди відносять захист від активних нападів, таких як відмова в обслуговуванні (DoS).
Секретність	Гарантувати, що інформація, яка може використовуватися для ідентифікації мережних пристроїв або ліній зв'язку, що беруть участь у мережному додатку, недоступна для неуповноваженого персоналу або пристроїв. Приклади такого типу інформації включають IP-адресу мережного пристрою та ім'я домену DNS. Наприклад, здатність ідентифікувати мережеві пристрої чи лінії зв'язку дає атакуючим цільову інформацію.

Захист площини кінцевого користувача рівня додатків полягає у захисті інформації користувача, що передається до мережі. Наприклад, конфіденційність ність номера кредитної картки користувача має бути захищена додатком електронної торгівлі. У таблиці 2.9 описуються цілі застосування вимірювань захисту рівня додатків в площині кінцевого користувача.

Таблиця 2.9

Застосування вимірювань захисту до рівня додатків у площині кінцевого користувача

Модуль 9: Рівень додатків, площина кінцевого користувача	
Вимірювання захисту	**Цілі захисту**
Управління доступом	Гарантувати, що лише уповноваженим користувачам та пристроям дозволено доступ до мережної програми та її використання.
Аутентифіка-ція	Перевірити особистість користувача або пристрою, який прагне отримати доступ до мережі та використовувати його. Як частина управління доступом можуть знадобитися методи автентифікації.
Збереженість інформації	Формувати звіт, що ідентифікує кожного користувача та пристрій, які отримали доступ до мережної програми та використовували її, а також дію, яка була виконана. Цей звіт повинен використовуватися як підтвердження доступу до мережі та його використання кінцевим користувачем або пристроєм.
Конфиденциій ність даних	Захищати дані кінцевого користувача (наприклад, номер кредитної картки користувача), які передаються, обробляються або зберігаються мережевим додатком, від несанкціонованого доступу та перегляду. Ті ж заходи вживаються стосовно даних користувача при передачі їх від користувача до мережі. Методи, що використовуються для керування доступом, можуть сприяти конфіденційності даних кінцевого користувача.
Безпека зв'язку	Гарантувати, що дані кінцевого користувача, які передаються, обробляються або зберігаються мережевим додатком, не змінюють напрями та не перехоплюються без санкціонованого доступу (наприклад, перехоплення) під час передачі між цими кінцевими точками. Ті ж заходи вживаються стосовно інформації користувача при передачі її від користувача до мережі.

Продовження таблиці 2.9

Цілісність даних	Захищати дані кінцевого користувача, які передаються, обробляються або зберігаються мережевим додатком від несанкціонованої модифікації, видалення, створення або дублювання. Ті ж заходи вживаються стосовно інформації користувача при передачі її від користувача до мережі.
Доступність	Гарантувати, що уповноважені кінцеві користувачі та пристрої не можуть бути позбавлені доступу до мережі. Сюди належить захист від активних нападів, таких як відмова в обслуговуванні (DoS), а також захист від пасивних нападів, таких як модифікація або видалення інформації про аутентифікацію кінцевого користувача (наприклад, ідентифікація користувача та його паролі).
Секретність	Гарантувати, що мережна програма не надає інформацію, яка стосується застосування програми кінцевим користувачем (наприклад, відвідані Web-сайти), неуповноваженому персоналу та пристроям. Наприклад, припустимо розкриття такого типу інформації лише персоналу правоохоронних органів, має ордер на обшук.

Висновок по розділу. Складовою безпеки інформації у локальній мережі ОІД є фізичний захист ОІД. Для цього використовуються технічна система охорони, система відео спостереження, СКУД. Визначені протидії загрозам інформації безпосередньо у ЛОМ ОІД. При побудові захищеної ЛОМ ОІД пропонуєтьться взяти за основу вимоги та положення Рекомендация МСЭ-Т X.805 - мережева архітектура захисту для забезпечення мережевого захисту. Аріхитектура може застосовуватися до різних мереж, де виникає питання сквозного захисту, незалежно від основної технології мережі.

РОЗДІЛ 3
КІБЕРНЕТИЧНА БЕЗПЕКА ЛОКАЛЬНОЇ МЕРЕЖІ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1. Показники якості комп'ютерної мережі

Згідно Серії Міжнародних Стандартів ISO 9000 якість - це сукупність властивостей системи, що дозволяють задовольняти потреби та очікування споживача [15]. Існують наступні основні показники якості комп'ютерних мереж.

1. Повнота виконуваних функцій. Мережа повинна забезпечувати виконання всіх передбачених для неї функцій щодо доступу до всіх ресурсів, по спільній роботі вузлів і по реалізації всіх протоколів і стандартів роботи.

2. Продуктивність - середня кількість запитів користувачів мережі, виконуваних за одиницю часу. Вона залежить від часу реакції системи на запит користувача. Це час складається з трьох складових:

- часу передачі запиту від користувача до вузла мережі, відповідального за його виконання;
- часу виконання запиту в цьому вузлі;
- часу передачі відповіді на запит користувача.

3. Пропускна здатність - важлива характеристика мережі, визначається обсягом даних, що передаються через мережу (або її ланки - сегменту) за одиницю часу. Часто використовується інша назва - швидкість передачі даних.

4. Надійність мережі - технічні характеристики, що характеризується середнім часом напрацювання на відмову.

5. Достовірність результантної інформації - це споживча характеристика мережі.

6. Безпека інформації в мережі є важливим її параметром, оскільки сучасні мережі мають справу з конфіденційною інформацією. Здатність мережі

захистити інформацію від несанкціонованого доступу і визначає ступінь її безпеки.

7. Прозорість мережі - це споживча характеристика, що означає невидимість особливостей внутрішньої архітектури мережі для користувача. Він повинен мати можливість звертатися до ресурсів мережі як до локальних ресурсів свого власного комп'ютера.

8. Масштабованість - це можливість розширення мережі без помітного зниження її продуктивності.

9. Універсальність мережі - можливість підключення до неї різноманітного технічного обладнання програмного забезпечення від різних виробників.

До складу цих показників якості мережі входять важливі технічні характеристики, які можуть бути оцінені і виражені кількісними значеннями вимірюваних або обчислюваних величин, а також оцінені суб’єктивно. До кількісних належать: продуктивність, пропускна здатність, надійність, достовірність інформації, безпека інформації.

У рамках даної роботи увага приділяється показнику безпеки інформації, конкретніше показник захищеності від несанкціонованого доступу. При оцінці якості захисту інформації від несанкціонованого доступу необхідно використовувати показники які враховують і порушення безпеки ресурсів у комп'ютерній мережі, і відновлення їх захищеного стану. Таким чином під таким показником буде розумітися коефіцієнт захищеності інформації від НСД.

Оцінку якості захисту інформації від несанкціонованого доступу у комп'ютерних мережах пропонується проводити у такій послідовності [16]:

1) збір та аналіз вихідних даних. При цьому визначаються: перелік вже захищених ресурсів; склад і технічні характеристики функціонування засобів захисту ресурсів; інтенсивності порушень безпеки ресурсів; інтенсивності відновлення захищеності ресурсів.

2) розрахунок показників захищеності окремих ресурсів.

3) побудова схем захищеності за типами загроз безпеці інформації;

4) розрахунок показників захищеності інформації у всій комп'ютерній мережі.

5) проведення оцінки якості захищеності інформації від НСД у мережі за обраним критерієм.

6) розробка рекомендацій Службі захисту інформації по забезпеченню потрібного рівня захисту інформації від НСД.

Детальніше по первому пункту. Вихідні дані при оцінки якості захисту інформації від НСД це наступні.

1) Перелік захищених ресурсів та де знаходяться.

2) Типи і характеристики функціонування засобів захисту ресурсів (кількість, де розташовані, що захищають ресурси, спосіб побудови захисту).

3) Інтенсивності порушень безпеки інформаційних ресурсів розраховуються окремо для трьох основних типів загроз інформаційній безпеці (загрози конфіденційності, цілісності та доступності.

4) інтенсивність відновлення захищеності ресурсів (в залежності від кількісного складу посадових осіб Служби захисту інформації; також розраховуються окремо для трьох основних типів загроз інформаційній безпеці).

Крім цього аналізуються: структура, параметри, алгоритми функціонування мережі.

Другим етапом є розрахунок показників захищеності. Пропонується використовувати наступні вирази:

$$K_{зах}^{к} = \frac{n_{вд}^{К}}{v^{К} + n_{вд}^{К}}, K_{зах}^{д} = \frac{n_{вд}^{д}}{v^{д} + n_{вд}^{д}}, K_{зах}^{ц} = \frac{n_{вд}^{ц}}{v^{ц} + n_{вд}^{д}}, \qquad (3.1)$$

де:

$K^{к}_{зах}, K^{ц}_{зах}, K^{д}_{зах}$ - коефіцієнти захищеності від загроз доступності, конфіденційності, цілісності;

$v^{k}, v^{ц}, v^{д}$ – інтенсивності порушень доступності, конфіденційності, цілісності;

$n^{К}_{вд}, n^{д}_{вд}, n^{ц}_{вд}$ - інтенсивності відновлення порушень доступності, конфіденційності, цілісності.

Оскільки в інформаційно-телекомунікаційних системах, у відповідності до нормативних документів захисту підлягають усі три критерії, та при допущенні, що порушення безпеки окремих ресурсів є незалежними подіями, використовуючи теорему множення для незалежних подій вираз (3.1) для усієї інформаційно-телекомунікаційної системи набуде вигляду:

$$K^{к,ц,д}_{зх\ імс} = \prod_{i=1}^{Y_р} K^{к,ц,д}_{зх\ i}$$

де:

$K^{к,ц,д}_{зх\ імс}$, коефіцієнт захищеності усієї інформаційно-телекомунікаційної системи;

$Y_р$ – кількість ресурсів, підлягають захисту;

$К^{к,ц,д}_{зх\ і}$ - коефіцієнт захищеності i – ого ресурсу.

3.2 Фізичний захист обчислювальної системи об’єкту інформаційної діяльності

Найбільш ефективний контроль здійснюється централізовано, вся інформація зберігається і обробляється в одному місці, а значить, слідкувати і налаштувати те, до якої її частини має доступ співробітник відповідно до своїх обов'язків, не складає труднощів.

Захист від витоків, як і будь-який підхід до безпеки повинен бути комплексним. Або ефективність буде така ж, як, вийшовши з будинку, закрийте двері на три замки, але залиште розпахнуті вікна. Перше, на що варто звернути увагу: понад 80% витоків відбуваються за необережністю, невмінням, помилкою або злого наміру співробітників компанії (інсайдерів).

Для захисту зовнішнього рубежу ОІД доцільно використовувати активні ІЧ засоби виявлення. Радіохвильовий небажано використовувати, тому що необхідною умовою коректної роботи радіохвильових сповіщувачів є відсутність поблизу радіопередавальних пристроїв.

В результаті дослідження існуючих засобів охорони для захисту зовнішнього рубежу ОІД доцільно використовувати активний ІЧ засіб виявлення та відеокамери.

Приблизний перелік засобів фізичного захисту ОІД наведено у таблиці 3.1.

Таблиця 3.1
Перелік продукції використаної в схематичному зображенні зовнішнього рубежу охорони приміщення за допомогою технічних засобів захисту

№ зп	Тип	Модель та виробник	Додаткова інформація
1	Відеокамера	SDI 560C	4 шт.
2	Прилад прийомо-контрольний	Дунай-4.2	1 шт.
3	Сповіщувач інфрачервоний	DD CROW SWAN GAD	2 шт.
4	Сповіщувач акустичний розбиття скла	Crow FW2-GBD-PRO	2 шт.
5	Відеореєстратор	Hikvision DS-7104NI-Q1	1 шт.

Для захисту внутрішнього рубежу ОІД доцільно використовувати пасивний інфрачервоний сповіщувач руху, сповіщувач руху та розбиття скла,

Магнітоконтактний сповіщувач, який входить в комплекс системи контролю доступу.

3.3. Мережева безпека

У базовому стеку протоколів Інтернет відсутні криптографічний захист та автентифікація передачі. Для забезпечення захисту передавання через Інтернет розроблено велику кількість різних протоколів, які працюють на різних рівнях: від прикладного до канального. Найзручнішими є протоколи мереженого рівня, оскільки їх використання не вимагає переписування програмних застосувань інших рівнів.

В основному використовуються наступні [17]:

Протокол S-HTTP. Призначений для створення захищених каналів на прикладному рівні, даючи змогу шифрувати повідомлення, причому кожне http-повідомлення шифрується окремо. Протокол передбачає попередню домовленість між відправником та одержувачем про параметри захищеного сполучення.

Протокол SSL (Secure Socket Layer). Це протокол сеансового рівня, надає сервіс створення захищених сеансів.

Призначений для вирішення завдань:

- розпізнавання сервера на запит клієнта. Це досить актуально при передачі конфіденційної інформації;
- розпізнавання клієнта на запит сервера;
- створення захищеного, зашифрованого сполучення. SSL складається з двох протоколів:
- Record protocol – визначає формати даних, які використовують для передавання;
- Handshake protocol – виконує процедуру взаємного розпізнавання.

Протокол PPTP (Point-to Point Tunneling Protocol). Розроблено фірмою Microsoft і широко використовується у її продуктах. Цей протокол інкапсулює кадри канального рівня у кадри IP, а на приймальному боці відбувається зворотний процес. Тобто між учасниками передавання ніби налагоджується пряме канальне сполучення, яке називають тунелем. Побічним ефектом такого тунелювання є те, що через такий тунель можна передавати пакети мереж, які не підтримують протоколів TCP/IP.

Технологія тунелювання є в основі створення віртуальних приватних мереж (Virtual Private Networks – VPN). VPN – це двопунктове сполучення, яке налагоджують у межах комутованої мережі через багато проміжних пристроїв і станцій. Передавання даних цим тунелем автентифікують та шифрують.

3.4. Підвищення безпеки інформації локальної мережі об’єкту інформаційної діяльності

Мережева безпека тісно пов'язана з управлінням IT-інфраструктурою: добре керовану мережу складніше зламати, ніж погано керовану. Для оцінки захищеності інформації ОІД необхідно проаналізувати наступне.

Що співробітники підключають до своїх комп'ютерів?

Які пристрої підключені всередині локальної мережі?

Яке програмне забезпечення використовується в інформаційній системі?

Чи налаштовані комп'ютери з урахуванням вимог інформаційної безпеки?

Як контролюється доступ співробітників до конфіденційної інформації?

Нижче перераховані різні безкоштовні або недорогі інструменти, а також процедури, які допоможуть відповісти на перераховані питання і підвищити рівень безпеки в організації. Перераховані інструменти не є вичерпними, але вони відображають широкий спектр доступних безкоштовних або недорогих інструментів, які можуть використовуватися для підвищення рівня інформаційної безпеки організації.

Пропонується використовувати поетапний підхід до побудови системи захисту інформації:

Етап 1 (безпека інфраструктури). Це необхідно для розуміння що знаходиться у мережі, і визначає базові вимоги щодо інформаційної безпеки.

Етап 2 (навчання співробітників). Приділяє увагу забезпеченню базових вимог безпеки і навчання співробітників питань інформаційної безпеки.

Етап 3 (реакція на інциденти). Необхідно щоб організації підготуватися до можливих інцидентів з інформаційної безпеки.

Безпека інфраструктури

На самому початку, щоб просунутися в питанні інформаційної безпеки, необхідно розібратися з локальною мережею, підключеними пристроями, критично важливими даними та програмами. Без чіткого розуміння того, що потрібно захистити, буде важко переконатися в тому, що забезпечується прийнятний рівень інформаційної безпеки.

Ключові моменти з цього питання:

1) Визначитися яку інформацію необхідно захищати?
2) Де у мережі зберігається найважливіша інформація?
3) Які пристрої підключені до вашої мережі?
4) Яке програмне забезпечення встановлено на ПЕОМ?

Яку інформацію необхідно захищати.

Щоб захистити конфіденційну інформацію, необхідно розуміти цінність її. Також необхідно визначити, яку інформацію потрібно захищати в рамках законодавства ,та діючих нормативних документів.

Які пристрої підключені до обчислювальної мережі

Якщо відомо які пристрої підключені до мережі, то така інфраструктура стає простіше в управлінні, і є розуміння які пристрої необхідно захищати. Нижче описані дії, які ви можете зробити, щоб дізнатися про пристрої у вашій мережі.

Яке програмне забезпечення встановлено на комп'ютерах ОІД.

Шкідливе програмне забезпечення у обчислювальній системі може створювати ризики, які необхідно мінімізувати, сюди ж можна віднести юридичну відповідальність за використання неліцензійного програмного забезпечення. Неоновлене програмне забезпечення є поширеною причиною проникнення шкідливого ПО, яке призводить до атак на інформаційні системи. Якщо відомо яке програмне забезпечення встановлено у обчислювальній мережі, є контроль за програмним забезпеченням яке встановлюється і є захист облікових записів з правами адміністратора, то зменшується ймовірність і вплив інцидентів інформаційної безпеки.

Дії:

Створити перелік додатків, веб-сервісів або хмарних рішень, які використовує організація. Необхідно обмежити число користувачів з правами адміністратора до мінімально можливого значення.

Використовувати складні паролі для адміністративних облікових записів, так як адміністратори можуть вносити серйозні зміни в систему.

Розробити процедуру встановки програмного забезпечення у обчислювальній мережі і заборонити встановку негативно схвалених компанією додатків за допомогою, наприклад, Applocker.

Навчання співробітників

Захист інформації вимагає не тільки технологічних рішень, а й обізнаності співробітників про запобігання випадкового порушення роботи ІТС. В рамках цього етапу не тільки буде описаний захист комп'ютерів, а й навчання співробітників важливим аспектам інформаційної безпеки.

Налаштування базових вимог з інформаційної безпеки

Для отримання доступу у інформаційну систему ОІД, шкідливі програми і зловмисники найчастіше використовують або небезпечно налаштовані додатки, або додатки з уразливостями. Необхідно переконатися, що операційна система і додатки (особливо веб-браузери) оновлені і правильно налаштовані. Крім того, рекомендується використовувати механізми захисту від шкідливих

програм, які можуть бути вбудовані в вашу операційну систему. Наприклад, Windows Device Guard, Windows Bitlocker і інші, згадані нижче.

Дії:

Періодично запускати сканер безпеки Microsoft Security Analyzer, щоб визначити, які патчі/оновлення не встановлені для операційної системи Windows, і які зміни в конфігурації необхідно виконати;

Переконуватися в оновленні браузерів і плагінів.

Використовувати антивірус з останніми оновленнями антивірусної бази для захисту систем від шкідливого ПЗ;

Обмежити використання знімних носіїв (USB, CD, DVD) тими співробітниками, кому це дійсно потрібно для виконання своїх службових обов'язків;

Встановити комп'ютерний інструмент Enhanced Mitigation Experience Toolkit (EMET) на комп'ютерах з Windows для захисту від вразливостей, пов'язаних з програмним кодом;

Використовувати багатофакторну автентифікацію там, де це можливо, особливо для віддаленого доступу до внутрішньої мережі або електронною поштою. Наприклад, використовувати безпечні токени / смарт-карти або смс повідомлення з кодами в якості додаткового рівня безпеки на додаток до паролів;

Користуватися шифруванням для безпечного віддаленого управління своїми пристроями та передачі конфіденційної інформації;

Розробка переоприятій по ІБ

Інформаційна безпека поєднує технології, процеси, людей. Недостатньо наявності тільки засобів захисту інформації. Щоб забезпечити безпеку організації, співробітники також повинні суворо дотримуватися вимог з інформаційної безпеки. Є два ключові чинники для навчання співробітників питанням інформаційної безпеки: донести інформацію до них, постійно підтримувати їх рівень знань.

Інформація, яку необхідно донести до співробітників:

Визначити співробітників організації, які мають доступ або обробляють конфіденційну інформації, і переконайтеся, що вони розуміють свою роль в захисті цієї інформації.

Двома найпоширенішими атаками є фішингові атаки по електронній пошті і по телефону. Переконатися, що співробітники можуть описати і визначити основні ознаки атаки. До таких ознак можуть відноситися ситуації, коли люди кажуть про терміновість, просять цінну або конфіденційну інформацію, використовують незрозумілі або технічні терміни, просять ігнорувати або обійти процедури безпеки.

Переконайтеся, що всі співробітники постійно оновлюють свої пристрої і програмне забезпечення.

Підтримка рівня знань:

Необхідно пояснювати співробітникам, як захистити організацію і переконуватися, що вони це розуміють;

Поширювате серед співробітників безкоштовні інформаційні матеріали з питань інформаційної безпеки.

Інструменти:

SANS Ouch! Інформаційний бюлетень , відео місяці, щоденні поради і плакати;

щомісячні інформаційні бюлетені MS-ISAC;

Реакція на інциденти

Після того, як організація розробила серйозний фундамент з інформаційної безпеки, необхідно вибудувати механізми реакції на інциденти. Такий підхід включає в себе розуміння, як справлятися з інцидентом інформаційної безпеки і як відновити роботу організації після нього.

Управління резервними копіями

Створення та управління резервними копіями може бути рутинним і не дуже цікавим завданням, однак, це один з кращих способів захистити

інформацію, відновитися після збою і повернути робочий процес у звичайне русло.

Дії:

Автоматично виконувати щотижневі резервні копії всіх комп'ютерів, що містять важливу інформацію;

Періодично перевіряти свої резервні копії, відновлюючи систему з використанням резервної копії;

Переконуватися, що, хоча б одна резервна копія недоступна по мережі. Це допоможе захистити від атак програм-вимагачів, оскільки дана резервна копія не буде доступна для шкідливого ПЗ.

Інструменти:

Microsoft «Створення резервної копії та відновлення»: утиліта резервного копіювання, вбудована в операційну систему Microsoft.

Apple Time Machine : інструмент резервного копіювання, встановлений в операційних системах Apple.

Amanda Network Backup : безкоштовний інструмент резервного копіювання з відкритим вихідним кодом.

Bacula: мережеве рішення для резервного копіювання та відновлення інформації з відкритим вихідним кодом.

Підготовка до інциденту

Ніхто не хоче, щоб стався інцидент, пов'язаний з інформаційною безпекою, але чим краща підготовленість, тим швидше зможемо відновитися після інциденту. До інцидентів з інформаційної безпеки відносять атаку типу «відмова в обслуговуванні», яка порушує доступ до вашого сайту, атаку програм-вимагачів, які блокують систему або дані, атаку шкідливим ПЗ.

Дії.

Визначити співробітників організації, які будуть приймати рішення і давати вказівки в разі інциденту.

Надайте контактну інформацію для IT-персоналу та / або сторонніх організацій.

Зберігати список зовнішніх контактів як частину свого плану. До них можуть відноситись юрисконсульти, страхові агенти, якщо ви застрахували ризики з інформаційної безпеки, консультанти з питань безпеки.

Необхідно ознайомитися з законами, пов'язаними з порушеннями в сфері інформаційної безпеки у країні.

Що робити, якщо стався інцидент:

Розглянути можливість звернення до консультанта з інформаційної безпеки, якщо характер і масштаб інциденту незрозумілий.

Розглянути можливість звернення до юриста, якщо виявиться, що в інциденті була скомпрометована конфіденційна інформація третьої сторони.

Підготуватися до повідомлення всіх порушених осіб, чия інформація була розкрита в результаті порушення.

Висновки до третього розділу:

В розділі описано методи забезпечення даних у мережах, рівні захисту інформаційних систем, з використанням яких розроблені рекомендації технічного захисту від витоків інформації та підвищення мережевої безпеки ОІД.

ВИСНОВКИ

Основною проблемою захисту інформації у локальних мережах є запобігання викраденню інформації.

В роботі проаналізовано загрози мережевій безпеці, та загрози власне інформації на об’єкті інформаційної діяльності.

Проаналізовано загальну архітектуру безпеки для відкритих систем разом з деякими видами архітектури, захисту мережевої інфраструктури. Встановлено, що існуючі рекомендації не у повній мірі відповідають викликам сьогодення в частині врахування людського фактору при забезпеченні безпеки інформації у локальній мережі об’єкту.

На підставі цього розроблені рекомендації для забезпечення інформаційної безпеки у локальній мережі об’єкта інформаційної діяльності з використанням мінімальних грошових затрат, та рекомендації як підвищити рівень безпеки без грошових затрат на вже існуючому підприємстві.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безпека інформаційно-комунікаційних систем М.В. Грайворонський, О.М. Новіков – К. : Вид.група BHV, 2009. – 608 с.

2. Костров, Д.В. Информационнаябезопасность в рекомендациях, требованиях, стандартах. 2008. В.Т. Шатун. Основи Менеджменту, 2006 Відкрита і закрита інформація [Електронний ресурс]: стаття. — Режим доступу до статті: http://management-books.biz

3. Закон України "Про інформацію" від 02.10.1992.

4. НД ТЗІ 2.2-006-08 Захист інформації на об’єкті інформаційної діяльності.

5. ДСТУ 3396.1.–96. Захист інформації. Порядок проведення робіт.

6. Загрози, атаки і способи їх відображення. – Доступний з http://alls.in.ua/5414-ip-telefoniya-zagrozi-ataki-i-sposobi-h-vidobrazhennya.html[Електронний ресурс]

7. Сигналізація. – Доступний з http://www.znanius.com/3798.html?&L [Електронний ресурс]

8. Андрончик А.Н. Защита информации в компьютерных сетях. - Екатеринбург: УГТУ-УПИ, 2008. – 248с.

9. Рекомендація ITU X.816 Інфраструктура забезпечення безпеки відкритих систем: основа перевірки безпеки і сигналів порушення безпеки. Та відповідний документ ISO/IEC 10181-7.

10. Рекомендація ITU X.805 Інформаційні технології - інформаційні об'єкти, які стосуються забезпечення безпеки, для контролю за доступом. Та відповідний документ ISO/IEC 15816.

11. Програма створення пакету комерційних пропозицій в сфері (відеоспостереження, СКУД, ОПВ) та електрики: https://s-p.zone[Електронний ресурс]

12. Кулаков Ю. О. Комп'ютерні мережі / Ю. О. Кулаков, Г. М. Луцький. — К.: Юніор, 2003. — 400 с.

13. Шаньгина В.Ф., Соколов А.В. Захист інформації в розподілених корпоративних мережах і системах. - Вид-во: ДМК, 2002. - 134 с.

14. Хмельов. Л. Оцінка ефективності заходів безпеки, які закладаються при проектуванні електронно-інформаційних систем. Праці науково-технічної конференції "Безпека інформаційних технологій", -Пенза, червень 2001.

15. Кудінов В.А. Аналіз ефективності Функціонування комплексних системи захисту відкритої информации в інформаційно-телекомунікаційній системе оперативного інформування.

16. Кисельов В.Д., Есиков О.В., Кислицин А.С. «Сучасні проблеми захисту в системах її передачі і обробки »/ Под ред. проф. Е.М. Сухарева. - М.: «Солід», 2000. - С. 200.

17. Татарникова Т.М. Захищені корпоративні мережі: завдання щодо захисту інформації. СПб: РГГМУ, 2012