Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістрський)
(рівень вищої освіти)

Розробка системи інформаційного захисту корпоративної мережі

(тема)

Виконав:

студент 2 курсу, групи *ІМІм-22-1*
Ніколаєнко Д.В.
(прізвище, ініціали)

Спеціальність 172 «*Телекомунікації та радіотехніка»*
(код і повна назва напряму підготовки)

Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма
«Інформаційно-мережна інженерія»
(повна назва освітньої програми)

Керівник *доц. Харченко Н.А.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Ніколаєнко Д.В.*
(підпис) (прізвище та ініціали)

Керівник _____ *Харченко Н.А.*
(підпис) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і повна назва)

Тип програми *освітньо-професійна*

Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Ніколаєнку Денису Віталійовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Розробка системи інформаційного захисту корпоративної мережі*

затверджені наказом університету від «*23*» *жовтня* 2023 року №*1233 Ст*

2. Термін подання студентом роботи до екзаменаційної комісії *11 січня 2024 р.*

3. Вихідні дані до роботи *проаналізувати різні типи засобів інформаційного захисту в сучасних корпоративних мережах, таких як криптографічний, мережний, транспортний, хмарний та апаратний; проаналізувати ризики та можливі атаки у корпоративних комп'ютерних мережах, розробити систему захисту інформації у корпоративній мережі, виконати відповідні налаштування системи VLAN та мережного маршрутизатору*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ

1. Базові поняття та принципи побудови сучасних комп'ютерних мереж

2. Аналіз сучасних загроз на інформаційні мережі

3. Розгляд різних засобів інформаційного захисту

4. Розробка інформаційного захисту корпоративної мережі

Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Слайди у форматі Power Point(назва, мета і задачі роботи, приклад схеми корпоративної мережі, види malware, принципи роботи та ієрархія DDoS-атак, види DDoS - атак, типи засобів інформаційного захисту, криптографічний захист, мережний захист, брандмауери, віртуальні приватні мережі (VPN), систем виявлення вторгнень (IDS) і запобігання вторгненням (IPS), план мережі з виділеними зонами комерційної таємниці, схема корпоративної локальної мережі VLAN на основі топології «зірка», транкування та створення групи VLAN, призначення веб-інтерфейсів до нього, включення комутаторів до access mode, базові налаштування маршрутизатора, основні результати роботи, висновки)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів атестаційної роботи	Строк виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*23.10.2023*	виконано
2	*Підбір літератури за темою роботи.*	*24.10-12.11.2023*	виконано
3	*Виконання розділу 1*	*13.11-27.11.2023*	виконано
4	*Виконання розділу 2*	*28.11-02.12.2023*	виконано
5	*Виконання розділу 3*	*03.12-15.12.2023*	виконано
6	*Виконання розділу 4*	*16.12-30.12.2023*	виконано
7	*Оформлення пояснювальної записки*	*01.01-11.01.2024*	виконано
8	*Оформлення презентаційного матеріалу,*	*12.01-14.01.2024*	виконано
	підготовка до захисту у ЕК		

Дата видачі завдання *23.10.2023 р.*

Студент _____ *(Ніколаєнко Д.В.)*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *(Харченко Н.А.)*

РЕФЕРАТ

Пояснювальна записка: 79 с., 36 рис., 24 джерел, 1 додаток

Об'єкт дослідження – корпоративні мережі, на які направлені різні види загроз.

Мета роботи – дослідження та розробка системи захисту корпоративних мереж від загроз.

Розглянуто потенційні ризики та наслідки загроз, проведено аналіз різних типів засобів інформаційного захисту в сучасних корпоративних мережах, розроблено системи захисту корпоративної мережі. У зв’язку з ростом кількості інформації, розробка системи захисту корпоративної мережі стає невід’ємною складовою для забезпечення цілісності інформації.

КОРПОРАТИВНА МЕРЕЖА, ТОПОЛОГІЯ, MALWARE, МЕТОДИ ЗАХИСТУ, ТРАФІК, IP-АДРЕСА, РОЗПОДІЛЕНА АТАКА, ШИФРУВАННЯ, HTTPS, ЛОКАЛЬНА МЕРЕЖА, VPN, ВИЯВЛЕННЯ І ЗАПОБІГАННЯ ВТОРГНЕННЯМ, SSH, IAM, БЕЗПЕКА НА ТРАНСПОРТНОМУ РІВНІ, БРАНДМАУЕР, РОЗРОБКА

THE ABSTRACT

Explanatory note: 79 pages, 36 figures, 24 source, 1 supplement

The object of follow-up - corporate networks that target by different types of threats.

The goal of the work - research and development of a system to protect corporate networks from threats.

The potential risks and consequences of threats are considered, various types of information security tools in modern corporate networks are analysed, and corporate network security systems are developed. Due to the growing amount of information, the development of a corporate network security system is becoming an integral part of ensuring the integrity of information.

CORPORATE LEVERAGE, TOPOLOGY, MALWARE, SECURITY METHODS, TRAFFIC, IP-ADRESS, DISTRIBUTED ATTACK. ENSRYPTION, HTTPS, LOCAL NETWORK, VPN, INTRUSION DETECTION AND PREVENTION, SSH, IAM, TRANSPORT LAYER SECURITY, FIREWALL, DEVELOPMENT

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

DoS – (Denial of Service) "відмова в обслуговуванні";

DDoS – (Distributed Denial of Service) розподілена "відмова в обслуговуванні;

ПЗ – програмне забезпечення;

ІС – інформаційна система;

ТЗ – технічні заходи;

СУБД – система управління базами даних;

IDS – (Intrusion Detection System) система виявлення вторгнень;

IPS – (Intrusion Prevention System) система запобігання вторгненням;

VPN – (Virtual Private Network) віртуальна приватна мережа;

AES – Advanced Encryption Standard;

DES – Data Encryption Standard;

SSL – Secure Socket Layer;

TLS – Transport Layer Security;

NIDS – виявлення вторгнень на основі мережі системи;

HIDS – система виявлення вторгнень на основі хоста;

CSP – постачальник хмарних послуг;

SSH – Secure Shell;

ВСТУП

На сучасному етапі розвитку електронного зв'язку, з ростом кількості інформації розробка системи інформаційного захисту корпоративної мережі стає невід’ємною складовою для забезпечення конфіденційності, цілісності та доступності цінної інформації. Запровадження такої системи стає вимогою часу, оскільки сучасні технології надають користувачам доступ до мережі з різних куточків світу, одночасно збільшуючи потенційні точки вразливості. Тому важливим є не лише реагування на поточні загрози, але і передбачення майбутніх та вдосконалення існуючих засобів захисту. Розробка ефективної системи інформаційного захисту включає в себе широкий спектр дій: від визначення стратегічних положень до розгортання технічних засобів, які гарантують безпеку та надійність корпоративної мережі. Існує необхідність у додатках і інструментах для забезпечення мережної безпеки, які можуть адаптуватися до сучасних викликів і забезпечувати захист інформації, незалежно від того, чи це особиста інформація користувача, чи важливі корпоративні дані. Тому, дисципліни криптографії, мережної, транспортної, хмарної та апаратної безпеки повинні розвиватися швидкими темпами, сприяючи виникненню новітніх інноваційних рішень і інструментів, що призводить до розробки практичних та легкодоступних додатків для забезпечення мережної безпеки.

1 БАЗОВІ ПОНЯТТЯ ТА ПРИНЦИПИ ПОБУДОВИ СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Сучасні корпоративні мережі

Корпоративна мережа - це складний комплекс взаємозв'язаних та погоджено функціонуючих програмних та апаратних компонентів, що забезпечує передачу інформації між різними видаленими застосуваннями та системами, використовуваними на підприємстві.

Корпоративні мережі називають також мережами масштабу підприємства. Мережі масштабу підприємства (корпоративні мережі) об'єднують велику кількість комп'ютерів на всіх територіях окремого підприємства. Вони можуть бути складно пов'язані та здатні покривати місто, регіон або навіть континент. Число користувачів і комп'ютерів може вимірюватися тисячами, а число серверів - сотнями, відстані між мережами окремих територій бувають такими, що доводиться використовувати глобальні зв'язки.

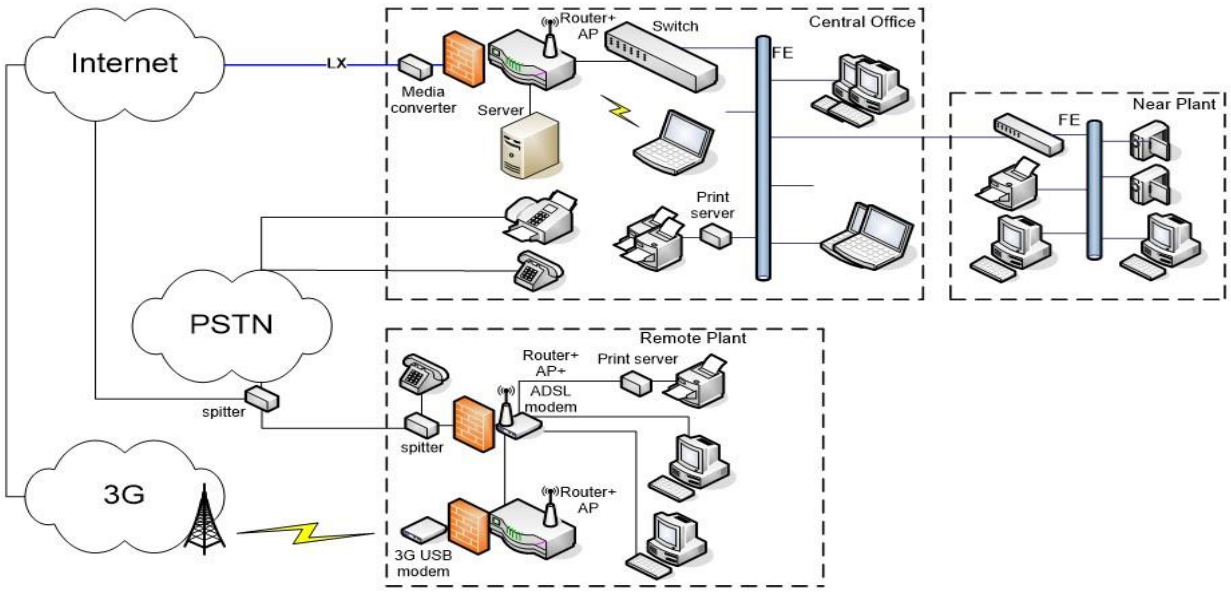

Рисунок 1.1 – схема корпоративної мережі

Корпоративну мережу необхідно розглядати у різних аспектах:

- структурному;

- системно-технічному;

- функціональному.

Зі структурної точки зору корпоративна мережа – мережа змішаної топології, в яку входять кілька локальних обчислювальних мереж. Для корпоративної мережі характерні:

- масштабність - тисячі комп'ютерів, сотні серверів, величезні обсяги даних, що зберігаються і передаються по лініях зв'язку, безліч різноманітних додатків;

- високий рівень гетерогенності - різні типи комп'ютерів, комунікаційного обладнання, операційних систем та додатків;

- використання глобальних зв'язків - мережі філій з'єднуються за допомогою телекомунікаційних засобів, зокрема телефонних каналів, радіоканалів, супутникового зв'язку.

З функціонального погляду корпоративна мережа – це ефективне середовище передачі актуальної інформації, яка потрібна на вирішення завдань корпорації.

Ієрархія корпоративних мереж- це ієрархічна структура мереж компаній являє собою складний механізм, що складається з декількох шарів, які постійно взаємодіють між собою. Всю систему можна представити у вигляді піраміди, складові якої розташовуються знизу вгору таким чином.

1. Комп'ютери, в яких зберігається і обробляється інформація.

2. Транспортна підсистема, за допомогою якої можна швидко пакетний канал доступу між комп'ютерами.

3. Шар мережних операційних систем, розташований над транспортною системою. Він відповідає за коректну роботу додатків в комп'ютерах і доставляє через транспортну систему в спільне користування ресурси комп'ютера.

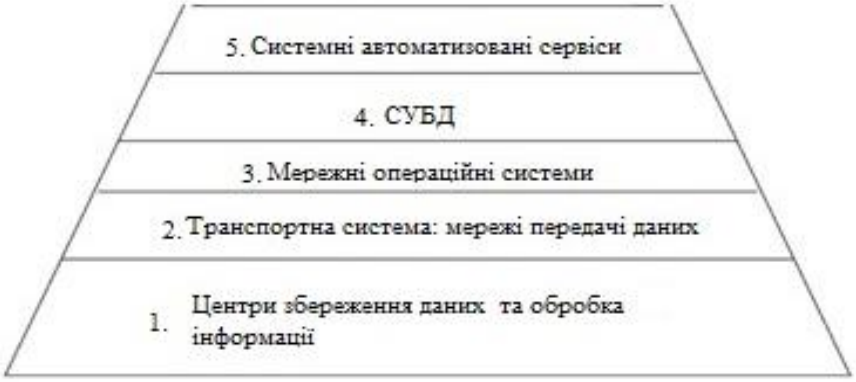

Рисунок 1.2 – ієрархічна структура корпоративної мережі

4. Наступним рівнем системи є системні сервіси корпоративної мережі, які використовують системи управління базами даних для пошуку інформації та надання її користувачам у зручному вигляді. До складу цих систем входить Інтернет, електронна пошта та інші корпоративні інструменти. Також вони зберігають їх у впорядкованому вигляді і дозволяють проводити з ними різні операції.

5. На останньому рівні піраміди розташовані специфічні системи, які виконують спеціальні завдання, необхідні для підприємства. До таких завдань можна віднести автоматизацію банківських систем, автоматизацію різних процесів і подібні операції.

1.2 Типи корпоративних мереж

Комп'ютерні та корпоративні мережі часто класифікуються за різними аспектами. А саме, за фунцією географічної області мережі, яку вони охоплюють, а також маштабністю та реалізацією топології, схему побудови мережі.

До функцій географічної області відносять такі мережі, як:

- LAN (Local-Area Network) – це локальна мережа, яка функціонує в межах

однієї будівлі, наприклад, будинку, офісу чи заводу (рис. 1.3). Локальні мережі широко використовуються для з'єднання персональних, офісних комп'ютерів і побутової електроніки, щоб вони могли спільно використовувати ресурси (наприклад, принтери) та обмінюватися інформацією;

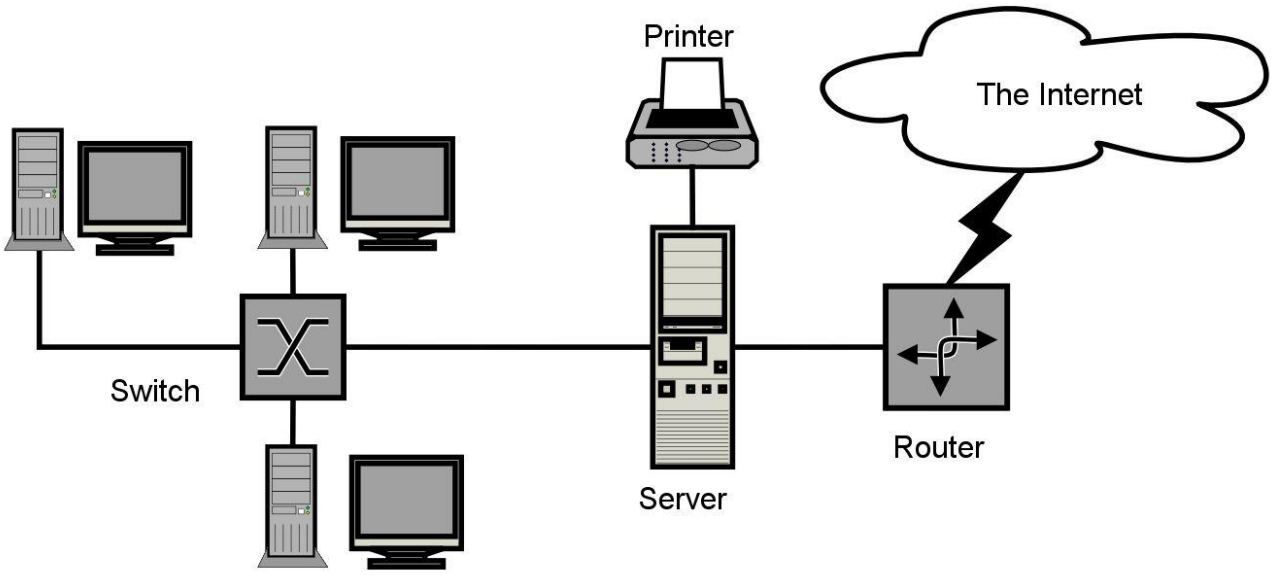

Рисунок 1.3 – Схема локальної мережі

- WLAN (Wireless Local-Area Network) – це бездротова локальна мережа, яка дуже популярна в наш час, особливо в будинках, старих офісних будівлях, кафетеріях та інших місцях. Використовується для зручності користування, або, де важко прокладати кабелі. Використовує стандарт для бездротових локальних мереж під назвою IEEE 802.11, відомий як WiFi;
- VLAN (Virtual Local Area Networks) – це віртуальна локальна мережа, яку можна визначити як набір портів, підключених до одного або декількох комутаторів Ethernet (рис. 1.4). Комутатор може підтримувати кілька VLAN, і він використовує один алгоритм навчання MAC-адресу для кожної віртуальної локальної мережі. Коли комутатор отримує кадр з невідомим або багатоадресним призначенням, він пересилає його на всі порти, які належать до однієї віртуальної мережі, але не через порти, які належать іншим віртуальним локальним мережам.

Аналогічно, коли комутатор дізнається адресу джерела на порту, він пов'язує її з віртуальною локальною мережею цього порту, і використовує цю інформацію тільки при переадресації кадрів у цій мережі [1];

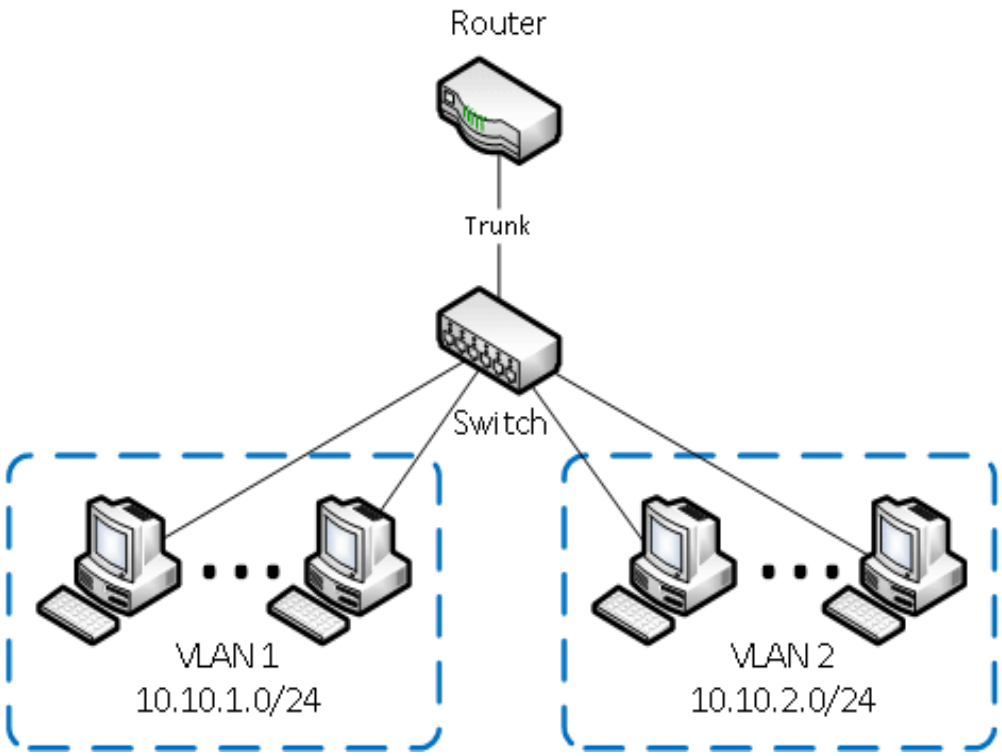

Рисунок 1.4 – Схема віртуальної локальної мережі

- MAN (Metropolitan Area Network) – це міська мережа, зазвичай з'єднує пристрої, що знаходяться на відстані до декількох десятків або сотень кілометрів один від одного (рис. 1.5). Найвідомішими прикладами MAN є мережі кабельного телебачення, які доступні в багатьох містах, та високошвидкісного бездротового інтернету, який був стандартизован як IEEE 802.16 і широко відомий як WiMAX.

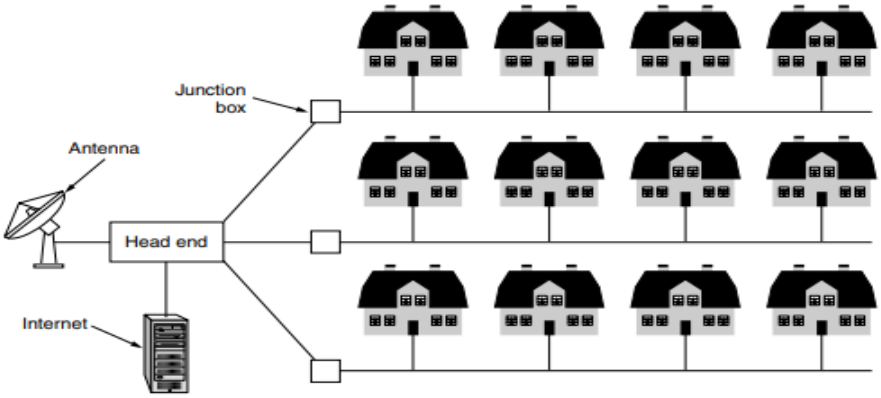

Рисунок 1.5 – Схема міської мережі (MAN)

- WAN (Wide Area Network) – це глобальна мережа, котра з'єднує хости, які можуть бути розташовані в будь - якій точці земної кулі. Охоплює велику географічну територію, часто країну або континент. Може включати в себе локальні та міські мережі.

Інша класифікація комп'ютерних мереж базується на їхній фізичній топології. Комп'ютерні мережі використовуються для того, щоб дозволити кільком хостам обмінюватися інформацією між собою.

Топологія повномаштабної сітчастої системи - іноді використовується, особливо, коли потрібна висока продуктивність і висока надмірність для невеликої кількості хостів (рис. 1.6). Однак вона має два основних недоліки:

- для мережі, що містить *n* хостів, кожен хост повинен мати *n*-1 фізичних інтерфейсів. Тому що, кількість фізичних інтерфейсів на вузлі буде обмежувати розмір повномасштабної мережі, яку можна побудувати;

- для мережі, що містить *n* вузлів, потрібно $\frac{n\times(n-1)}{2}$ з'єднань. Це можливо, коли є декілька вузлів в одній кімнаті, але рідко, коли вони розташовані на відстані кількох кілометрів один від одного [2].

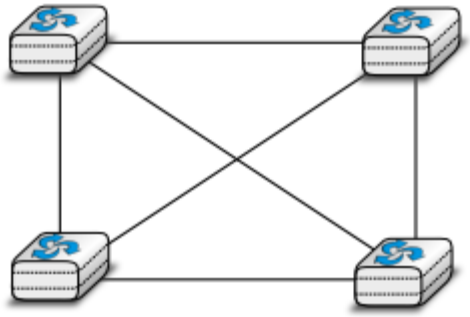

Рисунок 1.6 – Топологія повномаштабної сітчастої системи

Шина - фізична організація мережі, яка також використовується всередині комп'ютерів для з'єднання різних плат розширення (рис. 1.7). У шині всі вузли під'єднані до спільного середовища, як правило, кабелю через єдиний інтерфейс. Коли один комп'ютер посилає електричний сигнал по шині, сигнал приймається всіма комп'ютерами, підключеними до шини. Недоліком шинних мереж є те, що якщо шина фізично переривається, то мережа розділяється на дві ізольовані мережі. З цієї причини мережі на основі шини іноді вважаються складними в експлуатації та обслуговуванні, особливо коли кабель довгий і є багато місць, де він може обірватися. Така топологія на основі шини використовувалася в ранніх мережах Ethernet.

Рисунок 1.7 – Топологія «шина»

Зірка - це організація комп'ютерної мережі, яка має один фізичний інтерфейс, а між кожним вузлом і центром зірки існує одне фізичне з'єднання

(рис. 1.8). Вузол у центрі зірки може бути або частиною обладнання (комутатором), що підсилює електричний сигнал, або активним пристроєм (маршрутизатором), елементом обладнання, яке розуміє формат повідомлень, якими обмінюються через мережу. Вихід з ладу центрального вузла означає вихід з ладу всієї мережі. Однак, якщо виходить з ладу одне фізичне з'єднання (наприклад, через обрив кабелю), то відключається лише один вузол. Зіркоподібні мережі легші в експлуатації та обслуговуванні, ніж шиноподібні мережі. Адміністрування здійснюється за допомогою веб-інтерфейсу або через консольне з'єднання, центр зірки є головною точкою контролю.

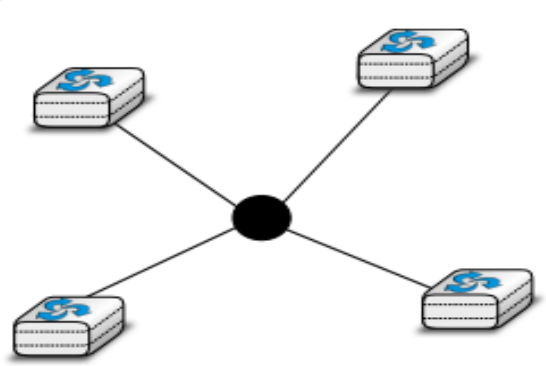

Рисунок 1.8 – Топологія «зірка»

Кільцева топологія. Подібно до організації шини, кожен хост має єдиний фізичний інтерфейс, що з'єднує його з кільцем (рис. 1.9). Будь-який сигнал, надісланий хостом на кільце, буде прийнятий усіма хостами підключеними до кільця. Єдине кільце не є найкращим рішенням, оскільки сигнал лише рухається в одному напрямку по кільцю; таким чином, якщо одна з ланок, що складають кільце, обривається, вся мережа виходить з ладу. У міських мережах кільця часто використовуються для з'єднання декількох локацій. В цьому випадку дві паралельні лінії, що складаються з різних кабелів, часто використовуються для резервування. За допомогою такого подвійного кільця, коли одне кільце виходить з ладу, весь трафік може бути швидко переключений на інше кільце.

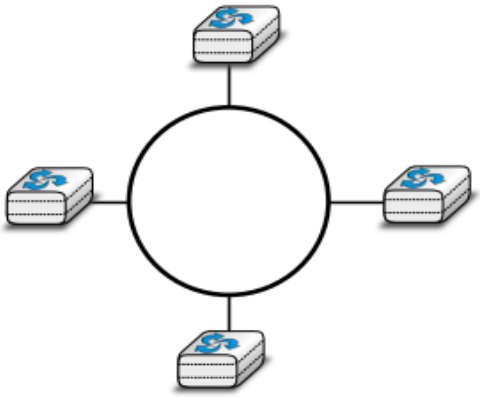

Рисунок 1.9 – Топологія «кільце»

Дерево - фізична організація мережі, зазвичай використовуються, коли необхідно підключити велику кількість клієнтів економічним та ефективним способом (рис. 1.10). Мережі кабельного телебачення часто організовані у вигляді дерева. На практиці більшість реальних мереж поєднують частину цих топологій. Наприклад, мережа кампусу може бути організована у вигляді кільця між головними будівлями, тоді як менші будівлі з'єднуються у вигляді дерева або зірки з головними будівлями [3].

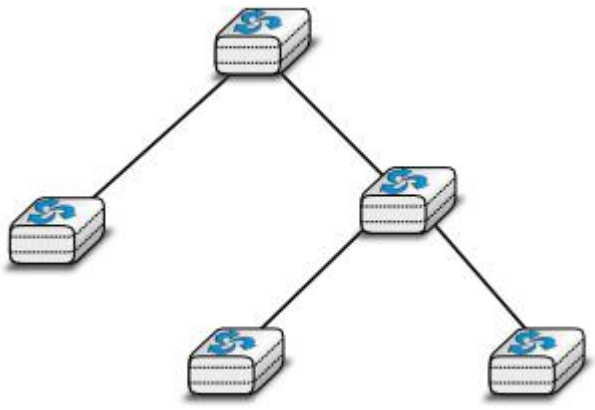

Рисунок 1.10 – Топологія «дерево»

2 АНАЛІЗ СУЧАСНИХ ЗАГРОЗ НА ІНФОРМАЦІЙНІ МЕРЕЖІ

2.1 Потенційні ризики та наслідки загроз

Всесвітня павутина дала бізнесу та суспільству великий прогрес у тому, як вони співпрацюють, спілкуються і як виглядають. Це також призвело до збільшення кількості шляхів розповсюдження шкідливого програмного забезпечення. Існує безліч видів атак на мережну інфраструктуру, які можуть впливати на конфіденційність, цілісність та доступність даних та сервісів.Тому треба вивчати та знати наслідки загроз.

Впровадження шкідливого коду на одному вузлі може викликати ланцюгову реакцію на всі вузли, доступних через мережу, в якій знаходиться вузол. Зважаючи на те, що організації та країни в значній мірі покладаються на мережні технології, комерційна цінність комп'ютерних мереж передбачає, що використання вразливості бізнес-мереж може завдати шкоди їхній роботі, а доступ до інтелектуальної власності та особистої інформації можуть отримати кіберзлочинці.

2.2 Види malware

Шкідливе програмне забезпечення визначається як будь-який код, доданий, змінений або видалений з програмної системи з метою навмисного завдавання шкоди або підриву функціонування системи [4]. Той факт, що шкідливе програмне забезпечення може спричинити втрату інформації, грошей, а також життя, становить велику загрозу для технологічного процесу.

Класифікація шкідливого програмного забезпечення залежить від характеристик виконання програм. Шкідливе програмне забезпечення також класифікується залежно від його корисного навантаження, від того, як воно експлуатує або робить систему вразливою. Аналізуючи шкідливі програмні

забезпечення, можна підтвердити припущення про те, який вид шкідливого забезпечення знаходиться у системі. З цією метою визначені категорії, на які поділяється більшість шкідливих програм:

Троянський кінь - це програма, яку зазвичай називають троянською, і яка представляється як легальне програмне забезпечення, але при завантаженні і виконується, вбудовує шкідливі підпрограми або файли на комп'ютері. У більшості випадків троянський кінь після запуску встановлює вірус або може не мати жодного корисного навантаження. Він не може самовідтворюватися і покладається на операторів системи для активації. Однак він може надати віддалений доступ зловмиснику, який потім може виконати будь-яку шкідливу дію, яка його цікавить. Програми-троянці по-різному впливають на комп'ютер, хост в залежності від прикріпленого до них корисного навантаження і, зазвичай, поширюються за допомогою соціальної інженерії [5].

Шпигунська програма (spyware) - це шкідлива програма, яка використовує функції операційної системи з метою шпигунства за діями користувача. Іноді вони мають додаткові можливості, такі як втручання в мережні з'єднання для зміни параметрів налаштування безпеки в зараженій системі. Вони поширюються, приєднуючись до легального програмного забезпечення, троянських коней або навіть використовуючи відомі вразливості програмного забезпечення. Шпигунські програми можуть стежити за поведінкою користувача, збирати натискання клавіш, звички користування інтернетом і надсилати цю інформацію автору програми.

Бекдор - шкідливий код, який встановлюється на комп'ютер, щоб надати зловмиснику доступ до комп'ютера. Зазвичай бекдори дозволяють зловмиснику підключатися до комп'ютера з практично без автентифікації та виконувати команди в локальній системі.

Ботнет - схожий на бекдор, оскільки дозволяє зловмиснику отримати доступ до системи, але всі комп'ютери, заражені одним ботнетом, отримують однакові інструкції з одного командно-контрольного сервера.

Malware – викрадач – це шкідливе програмне забезпечення, яке збирає інформацію з комп'ютера жертви і, зазвичай, надсилає її зловмиснику. Приклади включають сніфери, хеш-грабери паролів і кейлоггери. Це шкідливе програмне забезпечення зазвичай використовується для отримання доступу до онлайн-акаунтів, таких як електронна пошта або інтернет-банкінг.

Лаунчер (завантажувач) – це програма, що використовується для запуску інших шкідливих програм, це шкідливий код, який існує лише для завантаження іншого шкідливого коду. Зазвичай лаунчери використовують нетрадиційні методи для запуску інших шкідливих програм, щоб забезпечити непомітність або більший доступ до системи. Завантажувачі зазвичай встановлюються зловмисниками, коли вони вперше отримують доступ до системи.

Руткіт - це шкідливий код, призначений для приховування існування іншого коду. Руткіти зазвичай працюють у парі з іншими шкідливими програмами, такими як бекдор, щоб забезпечити віддалений доступ зловмиснику і ускладнити виявлення коду для жертви. Інструменти руткіту є дуже просунутими і складними, написані для того, щоб ховатися в легітимних процесах на зараженому комп'ютері, тому є дуже інвазивними і важкими для видалення. Вони розроблені таким чином, щоб здобути повний контроль над системою, та отримання найвищі привілеї на комп'ютері з-поміж інших можливих шкідливих дій. Через прийоми ухилення руткітів, більшість рішень постачальників безпеки не є ефективними у їх виявленні та видаленні, і тому їх виявлення та видалення покладається на ручні зусилля [6].

Програми залякування - призначені для того, щоб налякати інфікованого користувача і змусити його щось купити. Зазвичай має користувацький інтерфейс, який робить його схожим на антивірус або іншу програму безпеки. Вона повідомляє користувачам, що в їхній системі є шкідливий код, і що єдиний спосіб його позбутися – це купити їхнє "програмне забезпечення", хоча насправді програмне забезпечення, яке вони продають, не робить нічого, окрім видалення програми-лякалки.

Програми-вимагачі - це програми, які заражають комп'ютер або мережу і утримують систему в полоні, вимагаючи викуп від користувачів системи/мережі. Зазвичай програма шифрує файли або блокує систему так, щоб користувачі не мали до неї доступу. Потім вона відображає повідомлення, які змушують користувачів заплатити, щоб знову отримати доступ до своїх систем. Програми - вимагачі використовують ті ж засоби поширення, що й комп'ютерні черв'яки. а тому обізнаність користувачів та оновлення системи є важливими заходами запобігання.

Спамер – це шкідливе програмне забезпечення, яке заражає комп'ютер користувача, а потім використовує цей комп'ютер для надсилання спаму. Це шкідливе програмне забезпечення приносить дохід зловмисникам, оскільки дозволяючи їм продавати послуги з розсилання спаму.

Adware - це скорочення від Advertising Supported, що підтримується програмним забезпеченням, автоматично доставляє рекламу, яку бачать особливо у спливаючих вікнах на веб-сайтах та у програмному забезпеченні (рис. 2.1) [7].

Рисунок 2.1 – Результат зараження Adware

Більшість з них призначені для отримання прибутку рекламодавців. Деякі рекламні програми можуть постачатися в комплекті зі шпигунським програмним забезпеченням, що робить його дуже небезпечним, оскільки воно може відстежувати активність користувача активність користувача та викрадати інформацію про нього [7].

Хробак - це активна шкідлива програма, що самовідтворюється, яка може поширюватися мережею. Вона використовує цільові вразливості в операційній системі або встановленому програмному забезпеченні (рис. 2.2). Містить шкідливі підпрограми, але може використовуватися для відкриття каналів зв'язку які слугують активними носіями. Хробак споживає багато пропускної здатності та обчислювальних ресурсів через безперервне сканування і робить хост нестабільним, що може іноді призвести до краху системи. Він також може містити корисне навантаження, яке являє собою фрагменти коду, написані для впливу на комп'ютер шляхом крадіжки даних, видалення файлів, розсилання спаму або створення бота, який може призвести до того, що зробить заражену систему частиною бот-мережі [8]. У той час, як вірусам для поширення потрібна людська активність, хробаки мають здатність поширюватися і розмножуватися самостійно.

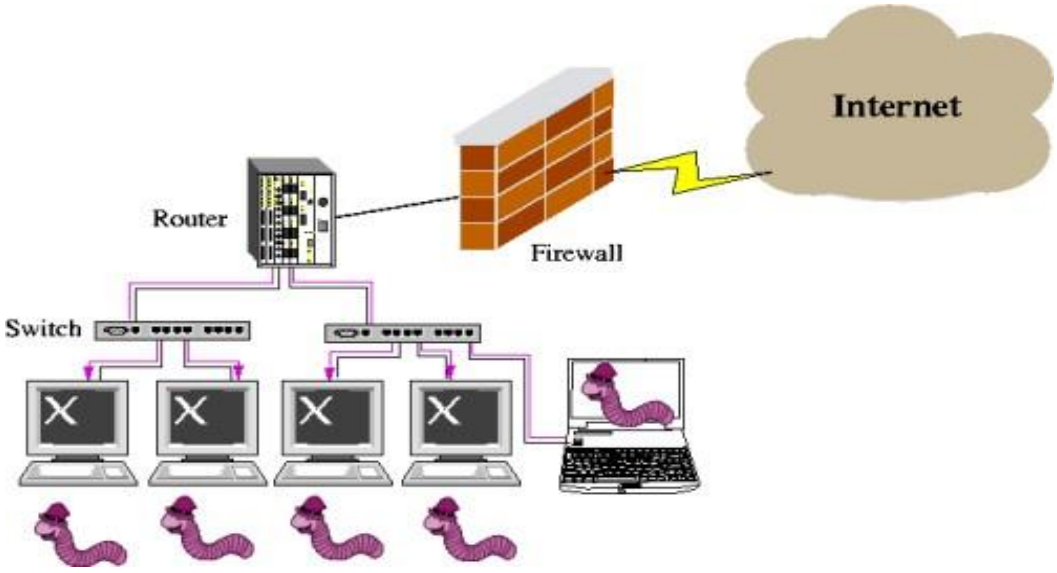

Рисунок 2.2 – Росповсюдження хробака на локальну мережу

Шкідливе програмне забезпечення також можна класифікувати на основі того, чи є мета зловмисника масовою або цілеспрямованою. Масові шкідливі програми, такі як програми для залякування, діють за принципом "дробовика" і призначене для ураження якомога більшої кількості комп'ютерів. З цих двох цілей, це найпоширеніша, і зазвичай менш складна, її легше виявити і захиститися від нього, оскільки програмне забезпечення для захисту націлене саме на нього.

Цільове шкідливе програмне забезпечення, як і унікальний бекдор, призначене для конкретної організації. Цільове шкідливе програмне забезпечення становить більшу загрозу для мереж, ніж масове шкідливе програмне забезпечення, тому що воно не є широко розповсюдженим, і ваші продукти безпеки, ймовірно, не захистять вас від нього. Без детального аналізу цілеспрямованого шкідливого програмного забезпечення майже неможливо захистити мережу від цього та видалити інфекції. Цільове шкідливе програмне забезпечення зазвичай дуже складне, і для його аналізу часто знадобляться просунут навичок аналізу.

2.3 Види DDOS-атак

Розподілена атака типу "відмова в обслуговуванні" (DDoS, абревіатура від англійської Distributed Denial of Service) - це зловмисна спроба порушити нормальний трафік цільового сервера, служби або мережі шляхом переповнення цілі або її інфраструктури потоком інтернет-трафіку.

DDoS-атака має ієрархічну структуру (рис. 2.3) – трирівневу модель, що складається з таких елементів:

- консолі управління, тобто головного комп'ютера, що подає сигнал у тому, що розпочалася атака;
- "комп'ютерів демонів", які, отримавши сигнал від консолі управління, передають його до «зомбованих» машин;

- атакуючих агентів – керованих заражених комп'ютерів, що посилають запити на кінцеву мету. Загальна схема ієрархічної структури DDoS-атаки зображено рис.2.3.

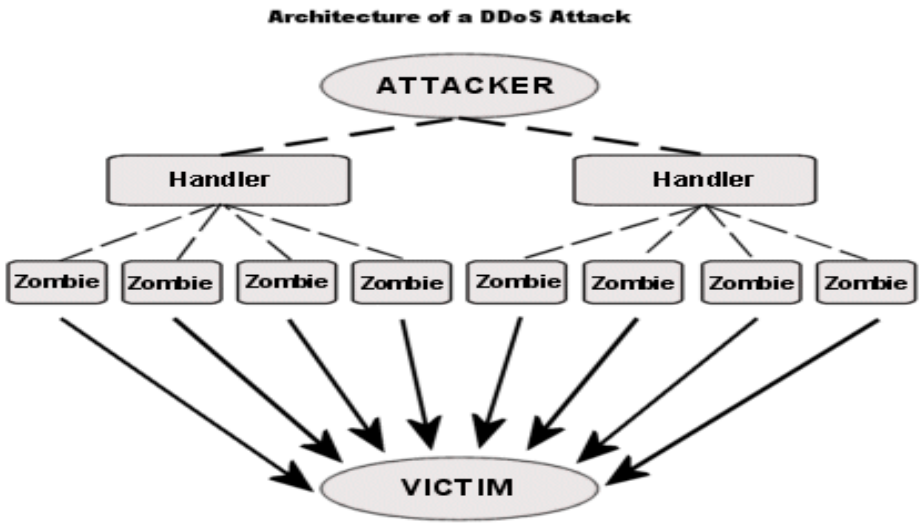

Рисунок 2.3 – Ієрархічна структура DDoS-атаки

Існує два основних типи атак, які викликають відмову в обслуговуванні:

Перший тип - призводить до зупинення всієї роботи системи або мережі. В цьому випадку системі надсилаються дані або пакети, які вона не очікує, і це призводить або до зупинки системи або до її перезавантаження. З точки зору зломщика ці атаки хороші тим, що за допомогою кількох невеликих витрат можна вивести систему з ладу, а щоб повернути її в нормальний режим, необхідно перезавантаження системи адміністратором. Таким чином, цей тип атак є найбільш руйнівним.

Другий тип **(**більш вживаний) - призводить до інформаційного переповнення системи або локальної мережі за допомогою великого трафіку, який неможливо обробити. За такої атаки зловмисник змушений постійно переповнювати систему пакетами, а в іншому випадку проведення атаки припиняється, і система відновлює нормальну роботу. Цей тип атаки вимагає більше зусиль з боку зломщика, проте відновлення системи вимагає

мінімального втручання адміністратора. При проведенні такої атаки, що зазнала нападу, машина отримує пакети одночасно від великої кількості машин, господарі яких самі можуть і не підозрювати про те, що відбувається. Крім того, оскільки ці атаки проводяться з широкого діапазону IP-адрес, набагато складніше блокувати і виявляти напад з тієї причини, що невелика кількість пакетів з кожної машини може не викликати реакції з боку систем виявлення вторгнень.

Типи DDoS-атак залежать від протоколу, яким здійснюється атака, наприклад HTTP (Hypertext Transfer Protocol), ICMP (Internet Control Message Protocol), UDP (User Datagram Protocol), TCP (Transmission Control Protocol), DNS (Domain Name System), SIP (Session Initiation Protocol). Розрізняють атаки по впливу на цільову жертву (пропускна здатність, пам'ять, процесор) та на скорочення послуг, що базується на помилках у програмному забезпеченні. Атаки можна розділити на два основні типи, флуд-атаки та логічні атаки.

1. Флуд-атаки - цей тип DDoS-атаки спрямований на перевантаження ресурсів сервера, таких як пропускна здатність, пам'ять або процесор, використовуючи велику кількість пакетів. Цей процес викликає відмову в обслуговуванні законних користувачів. Флуд-пакети зазвичай реалізуються через слабкі місця комунікаційних протоколів, тому більшість атак можуть мати назву, котра відповідає цим протоколам (TCP, UDP, ICMP, FTP, SIP чи HTTP) [9].

2. Логічні атаки спрямовані на слабкість додатків або програмного забезпечення на цільовому пристрої. Ці атаки використовують невелику кількість повідомлень, які протилежні атакам типу flooding. Мета полягає в тому, щоб привести пристрій у нефункціональний стан. До логічних атак можна віднести Ping смерті, атака Teardrop, атака "Земля" [10].

3 РОЗГЛЯД РІЗНИХ ЗАСОБІВ ІНФОРМАЦІЙНОГО ЗАХИСТУ

3.1 Типи засобів інформаційного захисту

Використання різних засобів інформаційного захисту грають критичну роль у сучасному цифровому світі, де конфіденційність та безпека інформації є найважливішими завданнями. До типів засобів інформаційного захисту можна віднести:

- криптографічний захист - захист використовує методи шифрування для захисту інформації від несанкціонованого доступу. Криптографічні алгоритми перетворюють дані в такий спосіб, що їх може розшифрувати лише особа з правильними ключами. Вони застосовуються в різних аспектах, включаючи захист даних в електронних листах, забезпечення безпеки платежів і захист конфіденційних інформаційних потоків;
- мережний захист - тип захисту, який зосереджений на захисті мережної інфраструктури від мережних атак та загроз. Він включає в себе використання брандмауерів, систем виявлення та запобігання вторгнення (IDS/IPS) і інших інструментів для моніторингу мережі і блокування потенційних загроз;
- транспортний захист - це тип інформаційного захисту системи, який забезпечує конфіденційність, цілісність та доступність даних під час їх передачі через мережі, забезпечує захист від перехоплення, зміни та підробки даних;
- хмарний захист – забезпечує безпеку в хмарних середовищах. Він включає в себе захист даних під час їх транспортування та зберігання в хмарі;
- апаратний захист - захист полягає в фізичному забезпеченні обладнання та інфраструктури від фізичних загроз. Це може включати в себе використання біометричних систем, систем контролю доступу та фізичного захисту приміщень з серверами і обладнанням.

Ці типи засобів інформаційного захисту можна використовувати окремо або спільно, залежно від конкретних потреб і загроз. А також, є засоби, які

можуть бути застосовані на інших рівнях протоколів TCP/IP, наприклад, браундмаєри.

3.2 Криптографічний захист

Криптографічний захист можна поділити на симетричну, асиметричну, квантову схеми шифрування. Але, до прикладу, розглянемо симетричну схему шифрування (рис. 3.1).

Існують дві вимоги для безпечного використання симетричного шифрування:

1) сильний алгоритм шифрування. Як мінімум, щоб алгоритм був таким, щоб зловмисник, який знає алгоритм і має доступ до одного або декількох зашифрованих текстів, не зміг би розшифрувати їх або підібрати ключ;

2) відправник і одержувач повинні отримати копії секретного ключа у безпечний спосіб і повинні зберігати ключ у безпеці. Якщо хтось може розкрити ключ і знає алгоритм, то вся комунікація з використанням цього ключа може бути прочитана.

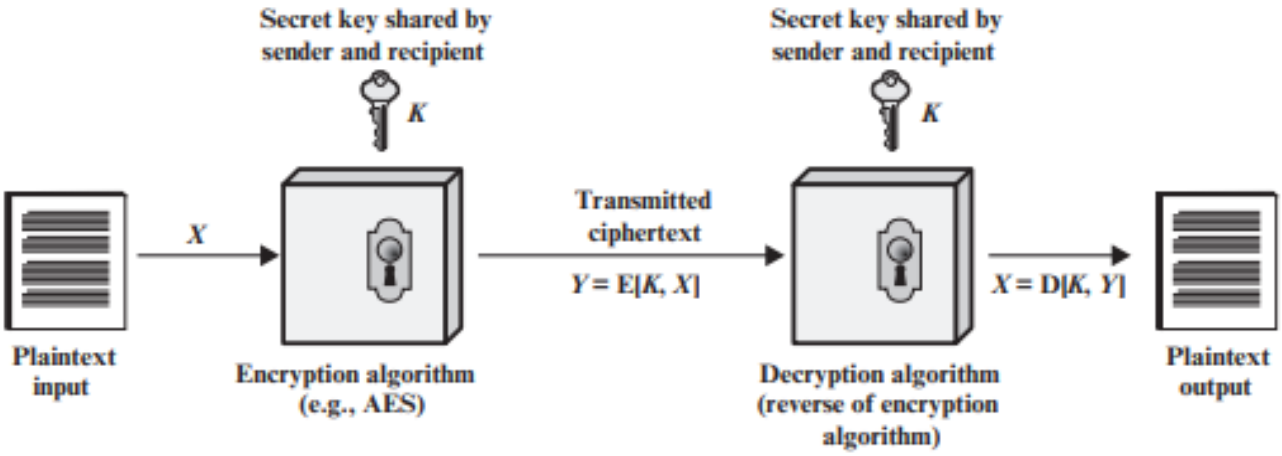

Рисунок 3.1 – спрощена модель симетричного шифрування

Безпека симетричного шифрування, в основному, залежить від секретності ключа, а не від секретності алгоритму. Тобто, непрактично розшифрувати повідомлення на основі зашифрованого тексту та знання алгоритму шифрування-розшифрування. Ця особливість симетричного шифрування робить його можливим для широкого використання. Той факт, що алгоритм не потрібно тримати в секреті, означає, що виробники можуть розробити недорогі реалізації алгоритмів шифрування даних.

Криптографічні системи зазвичай класифікуються за трьома незалежними вимірами:

1) тип операцій, що використовуються для перетворення відкритого тексту в зашифрований. Всі алгоритми шифрування ґрунтуються на двох загальних принципах: підстановки, при якому кожен елемент відкритого тексту відображається в інший елемент, і транспозиція, при якій елементи з відкритого тексту переставляються місцями. Фундаментальною вимогою є те, щоб інформація не була втрачена і процес операцій шифрування були оборотними. Більшість систем, які називаються продукційними системами, передбачають кілька етапів підстановок і транспозицій;

2) кількість використовуваних ключів. Якщо і відправник, і одержувач використовують один і той самий ключ, то система називається симетричною одноключовою з секретним ключем або звичайним шифруванням. Якщо відправник і одержувач використовують різні ключі, система називається асиметричною з двома ключами або шифруванням з відкритим ключем;

3) спосіб обробки відкритого тексту. Блоковий шифр обробляє вхідні дані по одному блоку елементів за раз, створюючи вихідний блок для кожного вхідного блоку. Потоковий шифр обробляє вхідні елементи безперервно, створюючи на виході по одному елементу за раз.

Data Encryption Standard (DES) – це застарілий стандарт шифрування 1977 року створення. Відкритий текст має довжину 64 біти, а ключ 56 біт, більші обсяги відкритого тексту обробляються 64-бітними блоками. Існує 16 раундів обробки при яких, з початкового 56-бітового ключа генерується 16 підключів, по

одному з яких використовується для кожного раунду. Процес розшифрування за допомогою DES по суті такий самий, як і процес шифрування. Правило шифрування та розшифрування полягає у наступному: застосовується зашифрований текст як вхідні дані, але у зворотньому порядку використовуються підключі K_i. Тобто, беруться K_{16} на першій ітерації, K_{15} на другій ітерації, і так далі, поки K_1 не буде використано на 16-й і останній ітерації [11].

Процес шифрування:

$$C = E(P, K) = E_{16}(E_{15}(\dots E_2(E_1(P, K_1), K_2) \dots), K_{16}) \quad (3.1)$$

Процес розшифрування:

$$P = D(C, K) = D_1(D_2(\dots D_{15}(D_{16}(C, K_{16}), K_{15}) \dots), K_1) \quad (3.2)$$

де E - функція шифрування;

D - функція розшифрування;

C - зашифрованный текст;

P - розшифрований текст;

K_i - ключі раунду.

Advanced Encryption Standard (AES) – це сучасний стандарт шифрування, який прийшов на заміну стандарту DES, використовує довжину блоку 128 біт і довжину ключа, яка може бути 128, 192 або 256 біт. Для опису взяли довжину ключа 128 біт, яка є найбільш поширеною. На вхід алгоритмів шифрування і дешифрування подається один 128-бітний блок. Цей блок копіюється в масив, який модифікується на кожному етапі шифрування або розшифрування. Після останнього етапу копіюється у вихідну матрицю. Аналогічно, 128-бітний ключ зображується у вигляді квадратної матриці байтів. Потім цей ключ розгортається у масив ключових слів. Кожне слово складається з чотирьох байтів, а загальний розклад ключа становить 44 слова для 128-бітного ключа. Впорядкування байт у

матриці відбувається за стовпчиками. Таким чином, перші чотири байти 128-бітового відкритого тексту, що подається на вхід шифру, займають перший стовпець матриці, другі чотири байти займають другий стовпчик, і так далі. Перші чотири байти розширеного ключа, які утворюють слово, займають перший стовпець матриці [11].

Більш детальне зображення алгоритму AES показано на рис. 3.2.

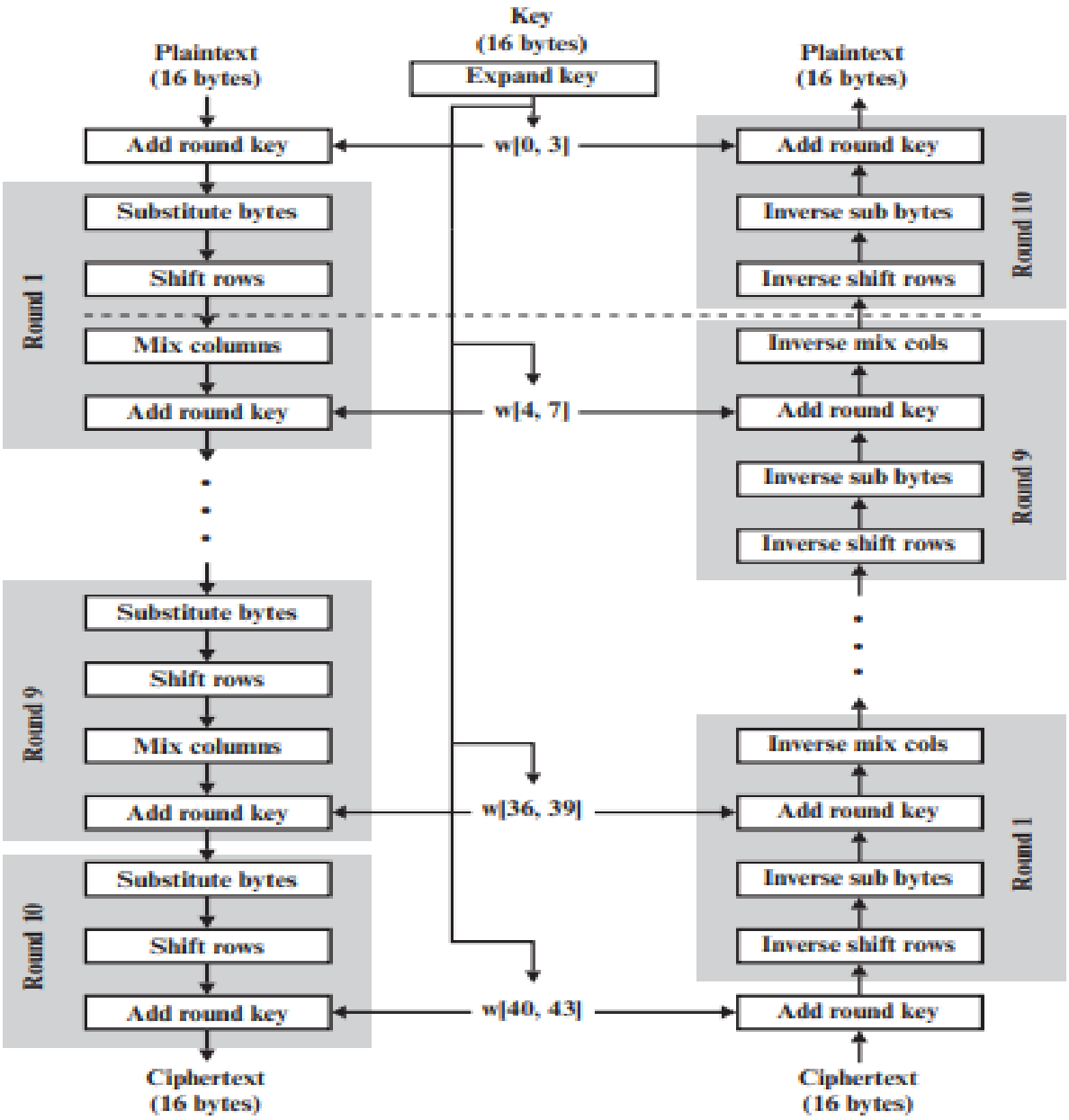

Рисунок 3.2 – детальний алгоритм шифрування та розшифрування у симметричному шифруванні за допомогою AES

Однією з важливих особливостей цієї структури є те, що вона не є структурою Фейстеля, як вищевикладений DES. У класичній структурі Фейстеля половина блоку даних використовується для модифікації іншої половини блоку, а потім половини міняються місцями. AES не використовує структуру Фейстеля, а обробляє весь блок даних паралельно під час кожного раунду, використовуючи підстановки та перестановки.

Ключ, який подається на вхід, розгортається у масив з сорока чотирьох 32-бітних слів, w[i]. Чотири окремих слова (128 біт) слугують ключем для кожного раунда.

Використовується чотири різних етапи, один з перестановкою і три з підстановкою:

- заміна байтів: використовується таблиця, яка називається S-боксом, для виконання побайтно заміни блоку;
- перестановка рядків: проста перестановка, яка виконується рядок за рядком;
- перемішування стовпців: заміна, яка змінює кожен байт у стовпчику як функцію від усіх байтів у стовпчику;
- додавання круглого ключа (round key): розраховується побітова логична операція XOR поточного блоку з частиною розширеного ключа.

Шифр починається з етапу додавання круглого ключа, за яким слідують дев'ять раундів, кожен з яких включає всі чотири етапи, після чого слідує десятий раунд, що складається з трьох етапів. Будь-який інший етап, застосований напочатку або в кінці, є оборотним, і тому не додає ніякої безпеки

Інші три етапи разом скремблюють біти, але самі по собі вони не забезпечують ніякої безпеки, оскільки вони не використовують ключ. Шифр можна розглянути як чергування операцій XOR-шифрування блоку, за яким слідує і саме скремблювання блоку,а за яким слідує шифрування XOR, і так далі. Ця схема є ефективною і безпечною.

Кожен етап є легко оборотним. Для етапів Substitute Byte, Shift Row та Mix Columns в алгоритмі розшифрування використовується обернена функція. Для

етапу додавання круглого ключа, інверсія досягається шляхом XOR-обернення того ж самого круглого ключа з блоком, використовуючи результат, що A ⊕ B ⊕ B = A, де A - це блок тексту, а B - це круглий ключ.

Як і у більшості блокових шифрів, алгоритм розшифрування використовує розширений ключ у зворотному порядку. Однак, алгоритм розшифрування не є ідентичний алгоритму шифрування. Це є наслідком особливої структури AES.

3.3 Мережний захист

Мережний захист складається зі служб безпеки, моніторингу та захисту базових служб ресурсів. Безпека включає брандмауери (Firewalls), віртуальні приватні мережі (VPN), управління та запобігання вторгнень (Intrusion Detection and Prevention Systems, IDS/IPS), що можуть разом створювати комплекс захисту, такий як захист від розподілених атак відмови в обслуговуванні (DDoS). Багато інших служб ще можна перерахувати в цьому розділі, наприклад, управління ідентифікацією і доступом, захист від втрати даних, це також вносить свій внесок в захист мережі.

3.3.1 Брандмауери

Брандмауери (firewalls) – це засіб захисту периметра, що захищає внутрішню мережу від зовнішніх загроз (рис. 3.3). Брандмауер вибірково дозволяє або блокує вхідний і вихідний трафік.

Брандмауери можуть бути окремими мережним пристроями, розташованими на вході в приватну мережу, або персональними програмами-брандмауерами, що працюють на персональних комп'ютерах. Брандмауер організації захищає внутрішню спільноту; персональний брандмауер може бути налаштований відповідно до потреб окремої людини. Брандмауери можуть забезпечити поділ та ізоляцію між різними мережевими зонами (рис. 3.4), а саме: загальнодоступним Інтернетом, приватними інтрамережами та демілітаризованою зоною (ДМЗ) [12].

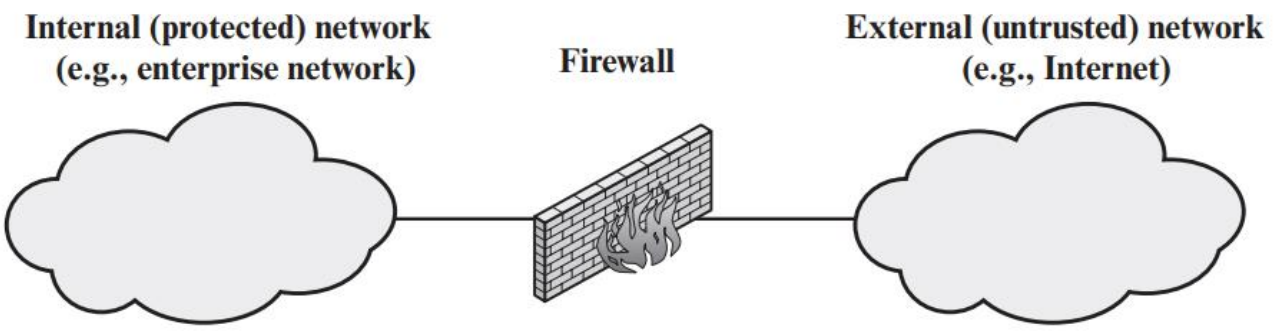

Рисунок 3.3 – Загальна модель firewall

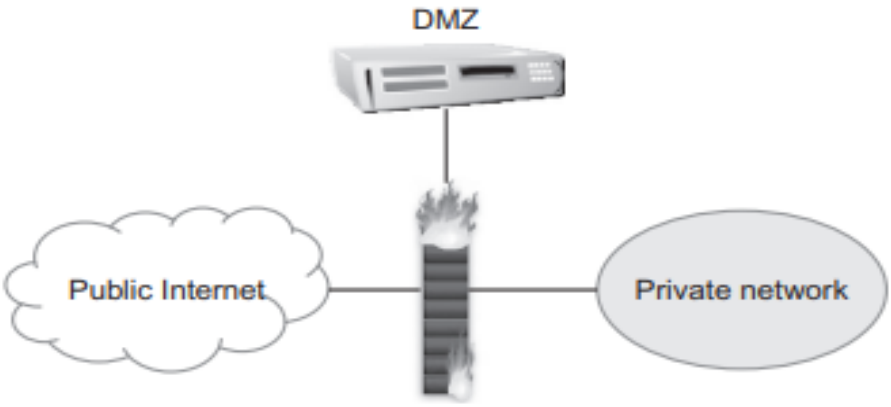

Рисунок 3.4 – Контроль брандмауером різних мережних зон

Брандмауер може контролювати мережний трафік на різних рівнях, від низькорівневих мережних пакетів окремо, або в складі потоку, до всього трафіку в межах транспортного з'єднання, аж до перевірки деталей протоколів додатків. Вибір відповідного рівня визначається бажаною політикою доступу брандмауера. Він може працювати як позитивний фільтр, пропускаючи тільки пакети, що відповідають певним критеріям, або як негативний фільтр, відкидаючи будь-який пакет, який не відповідає певним критеріям. Критерії реалізують політику доступу для брандмауера. Залежно від типу брандмауера, він може перевіряти один або декілька заголовків протоколів у кожного пакета, корисне навантаження кожного пакета або шаблон, згенерований послідовністю пакетів.

Packet Filtering Firewall або брандмауер з фільтрацією пакетів застосовує набір правил до кожного вхідного і вихідного IP, а потім пересилає або відкидає їх. Зазвичай брандмауер налаштовується на фільтрацію пакетів, що йдуть в обох напрямках (з і до внутрішньої мережі і до внутрішньої мережі) [13].

Правила фільтрації ґрунтуються на інформації, що міститься в мережному пакеті:

- IP-адреса джерела: IP-адреса системи, яка створила IP-пакет (наприклад, 192.178.1.1);
- IP-адреса призначення: IP-адреса системи, до якої IP-пакет намагається досягти (наприклад, 192.168.1.2);
- адреса транспортного рівня джерела та призначення: Номер порту транспортного рівня (наприклад, TCP номер порту транспортного рівня (наприклад, TCP або UDP), який визначає такі програми, як SNMP або TELNET;
- поле IP-протокол: визначає транспортний протокол;
- інтерфейс: для брандмауера з трьома або більше портами, з якого інтерфейсу брандмауера надійшов пакет, або для якого інтерфейсу брандмауера цей пакет призначений.

Фільтрація пакетів зазвичай налаштовується як список правил, заснованих на збігах з полями в IP або TCP заголовку. Якщо є збіг з одним з правил, це правило викликається щоб визначити, чи переслати або відкинути пакет. Якщо немає збігу з жодним то виконується дія за замовчуванням.

Можливі дві політики за замовчуванням:

- за замовчуванням = відкинути: те, що явно не дозволено, заборонено;
- за замовчуванням = переслати: те, що явно не заборонено, дозволено.

Політика відхилення за замовчуванням є більш консервативною. Спочатку все блокується, а служби потрібно додавати у кожному конкретному випадку. Ця політика більш помітна користувачам, які, швидше за все, сприйматимуть брандмауер як перешкоду. Однак, саме цій політиці, швидше за все, віддадуть перевагу підприємства та урядові організації. Крім того, видимість для користувачів зменшується в міру створення правил. Політика переадресації за

замовчуванням підвищує простоту використання для кінцевих користувачів, але знижує рівень безпеки; адміністратор безпеки повинен, по суті, реагувати на кожну нову загрозу безпеці, коли про неї стає відомо.

Stateful Inspection Firewalls або брандмауер з перевіркою стану приймає рішення про фільтрацію на основі окремих пакетів і не бере до уваги контекст вищого рівня. Більшість стандартизованих додатків, які працюють поверх TCP, працюють за моделлю клієнт-сервер. Наприклад, для простого протоколу передачі електронної пошти протоколу (SMTP), електронна пошта передається від клієнтської системи до серверної. Клієнтська система генерує нові повідомлення електронної пошти, як правило, на основі даних, введених користувачем. Система-сервер приймає вхідні повідомлення електронної пошти і поміщає їх у відповідні поштові скриньки користувачів. SMTP працює шляхом встановлення TCP-з'єднання між клієнтом і сервером, в якому номер порту TCP-сервера, який ідентифікує програму SMTP-сервера, дорівнює 25. SMTP-сервер, дорівнює 25. Номер порту TCP для клієнта SMTP - це число між 1024 до 65535, яке генерується SMTP-клієнтом.

Загалом, коли програма, яка використовує TCP, створює сеанс зв'язку з віддаленим хостом, він створює TCP-з'єднання, в якому номер порту TCP для віддаленого (серверної) програми є числом, меншим за 1024, а номер порту TCP для локальної (клієнтської) програми є числом у діапазоні від 1024 до 65535. Числа, менші за 1024 є "відомими" номерами портів і призначаються назавжди для певних програм (наприклад, 25 для серверного SMTP). Номери від 1024 до 65535 генеруються динамічно і мають тимчасове значення лише на час існування TCP-з'єднання. Простий брандмауер з фільтрацією пакетів повинен дозволяти вхідний мережевий трафік на всі ці порти з високими номерами для трафіку на основі TCP. Це створює вразливість, якою можуть скористатися неавторизовані користувачі.

Брандмауер з перевіркою стану пакетів посилює правила для TCP-трафіку шляхом створення каталогу вихідних TCP-з'єднань. У цьому каталозі є запис для кожного поточного встановленого з'єднання. Тепер пакетний фільтр буде

пропускати вхідний трафік на порти з високими номерами лише для тих пакетів, які відповідають профілю одного із записів у цьому каталозі.

Брандмауер з перевіркою пакетів перевіряє ту саму інформацію про пакети, що і брандмауер з фільтрацією пакетів, але також записує інформацію про TCP-з'єднання. Деякі брандмауери зі збереженням стану також відстежують порядкові номери TCP, щоб запобігти атакам, наприклад, перехоплення сеансу. Деякі з них навіть перевіряють обмежену кількість даних додатків для деяких відомих протоколів, таких як FTP, IM і команди SIPS, щоб ідентифікувати і відстежувати пов'язані з ними з'єднання (рис. 3.5).

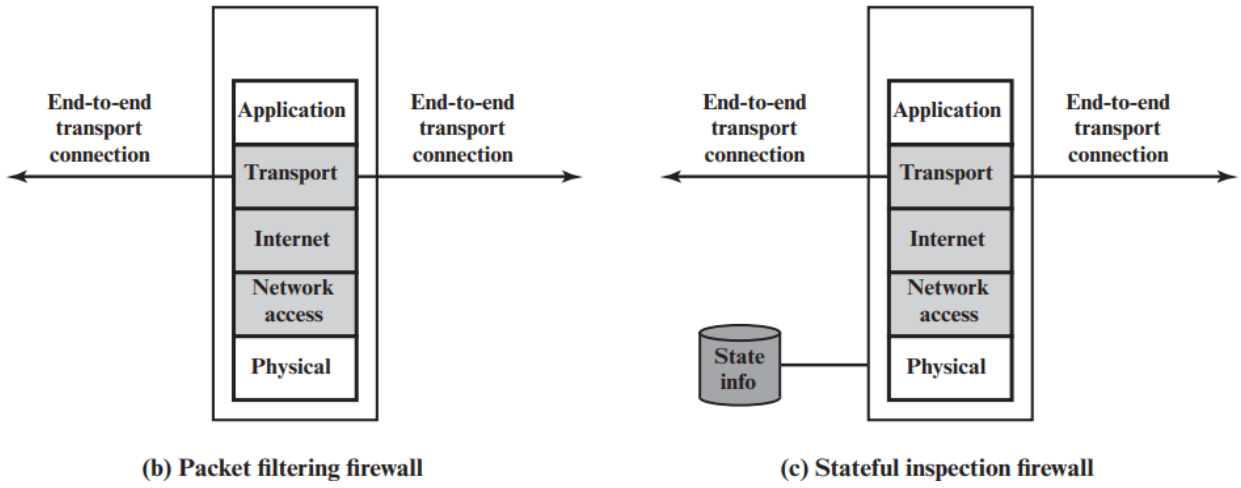

Рисунок 3.5 – Типи брандмауерів: b) з фільтрацією пакетів, c) з перевіркою стану

3.3.2 Проксі

Application proxy або шлюз на рівні додатків, діє як ретранслятор трафіку. Користувач звертається до шлюзу за допомогою програми на основі протоколу TCP/IP, наприклад, Telnet або IP-додаток, і шлюз запитує у користувача ім'я віддаленого хоста, до якого потрібно отримати доступ. Коли користувач відповідає і надає дійсний ідентифікатор користувача та інформацію для автентифікації, шлюз зв'язується з додатком на віддаленому хості і передає сегменти TCP, що містять дані програми, між двома кінцевими точками. Якщо

шлюз не реалізує код проксі-сервера для певної програми, сервіс не підтримується і не може бути перенаправлений через брандмауер. Крім того, шлюз можна налаштувати на підтримку лише певних функцій програми, які мережний адміністратор вважає прийнятними, одночасно забороняючи всі інші функції. Шлюзи на рівні додатків, як правило, більш безпечні, ніж пакетні фільтри. Замість того, щоб намагатися впоратися з численними можливими комбінаціями, які повинні бути дозволені і заборонені на рівні TCP і IP, шлюзу прикладного рівня потрібно лише ретельно перевіряти лише кілька дозволених додатків. Крім того, легко реєструвати і перевіряти весь вхідний трафік на рівні додатків. Основним недоліком цього типу шлюзу є додаткова обробка накладні витрати на кожне з'єднання. По суті, між кінцевими користувачами існує два зрощених з'єднання кінцевими користувачами, причому шлюз знаходиться в точці з'єднання, а шлюз повинен перевіряти і перенаправляти весь трафік в обох напрямках.

Circuit-level proxy або проксі-канальний рівень. Це може бути автономна система або спеціалізована функція що виконується шлюзом на рівні додатків. Як і у випадку з application proxy, шлюз канального рівня не дозволяє наскрізне TCP-з'єднання; скоріше, шлюз встановлює два TCP-з'єднання, одне між собою і користувачем TCP на внутрішньому хості, і одне між ним і користувачем TCP на зовнішньому хості. Після встановлення двох з'єднань шлюз, як правило, ретранслює TCP-сегменти від одного з'єднання до іншого без перевірки вмісту (рис. 3.6).

Функція безпеки полягає у визначенні того, які з'єднання будуть дозволені. Типове використання шлюзів канального рівня - це ситуація, коли системний адміністратор довіряє внутрішнім користувачам. Шлюз може бути налаштований на підтримку прикладного рівня або проксі-сервісу для вхідних з'єднань і функцій канального рівня для вихідних з'єднань. У такій конфігурації шлюз може нести витрати на обробку накладні витрати на перевірку вхідних даних програми на наявність заборонених функцій, але не але не несе таких витрат на вихідні дані [14].

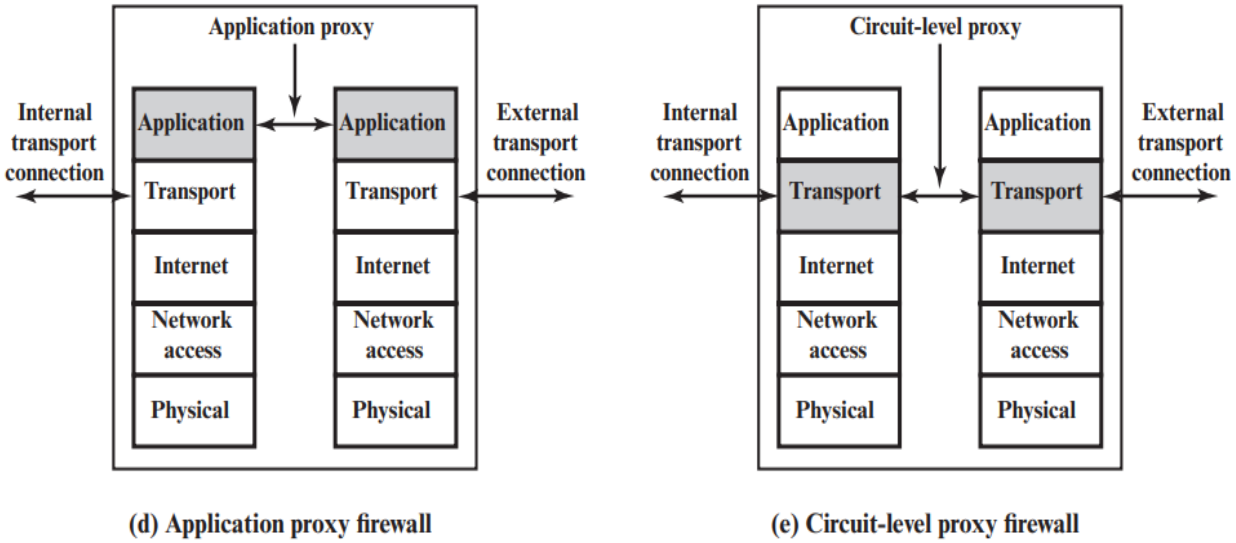

Рисунок 3.6 – Типи брандмауерів: d) шлюз на рівні додатків, e) проксі-канальний рівень

3.3.3 Віртуальні приватні мережі

Віртуальні приватні мережі (VPN) - це комунікаційне середовище, в якому доступ контролюється, щоб дозволити з'єднання тільки в межах визначеної спільноти інтересів, і побудоване за допомогою певної форми розділення загального базового середовища зв'язку, де це базове середовище зв'язку надає послуги мережі на невиключній основі.

Віртуальні приватні мережі можна налаштувати так, щоб весь трафік між пристроями та мережею організації проходив через VPN. Для обмеження доступу з пристрою до ресурсів організації слід використовувати надійний протокол автентифікації пристрою до ресурсів організації. Часто пристрій має єдиний автентифікатор, оскільки передбачається, що пристрій має лише одного користувача. Кращою стратегією є дворівневий механізм автентифікації, який передбачає автентифікацію пристрою, а потім автентифікацію користувача пристрою. Приклад роботи VPN зображено на рис. 3.7.

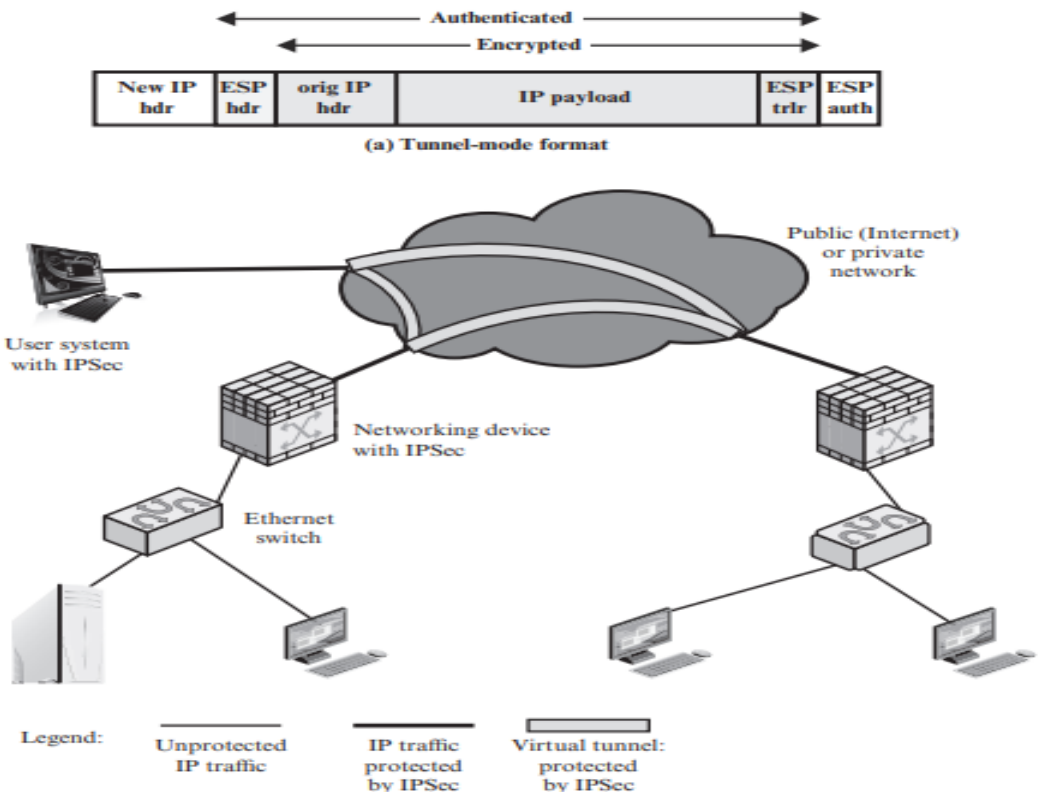

Рисунок 3.7 – Сценарій VPN через IPsec

Насправді існує декілька різних типів VPN, і в залежності від функціональних вимог, існує декілька різних методів побудови кожного типу VPN. Процес вибору повинен включати в себе розгляд проблеми, аналіз ризиків, пов'язаних з безпекою, що забезпечується конкретною реалізацією, питання масштабування при збільшенні розміру VPN, а також складність, пов'язану як з реалізацією VPN, так і з постійним обслуговуванням та усуненням несправностей.

Для спрощення опису різних типів VPN, вони були розділені на категорії, які знаходяться на різних рівнях набору протоколів TCP/IP (рис. 3.8), типи VPN розглянемо на мережному та транспортному рівні [15].

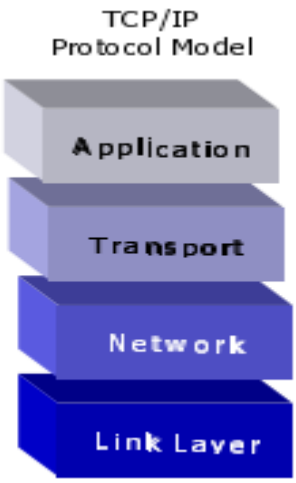

Рисунок 3.8 – Різні рівні набору протоколів TCP/IP

Мережний рівень у наборі протоколів TCP/IP складається з системи IP-маршрутизації - способу передачі інформації про доступність з однієї точки мережі до іншої. Існує декілька методів побудови VPN на мережному рівні: "однорангових" і "оверлейних" VPN. Однорангова (Peer-to-Peer) модель VPN - це модель, в якій обчислення шляху переадресації на мережному рівні виконується покроково, де кожен вузол на проміжному шляху передачі даних є одноранговим з наступним вузлом. Традиційні маршрутизовані мережі є прикладами "однорангових" моделей, де кожен маршрутизатор на маршруті мережі є одноранговим зі своїми сусідніми вузлами. Альтернативно, "оверлейна" модель VPN - це модель, в якій мережний рівень пересилання не здійснюється на основі "hop-by-hop"(принцип обробки інформації), а скоріше, мережа проміжного канального рівня використовується як "прохідний шлях" до іншого граничного вузла на іншій стороні великої хмари.

Прикладами "оверлейних" моделей VPN є IPsec (IP Security), частково можна віднести SSL (Secure Socket Layer), і тунелювання. Про відмінності між одноранговими і оверлейними моделями, слід зазначити, що оверлейна модель вносить деякі серйозні проблеми з масштабуванням у випадках, коли потрібна велика кількість вихідних однорангових вузлів. Це пов'язано з тим, що кількість суміжності зростає в прямій залежності від кількості однорангових вузлів -

обсягу обчислювальних і продуктивних накладних витрат, необхідних для підтримки стану маршрутизації, інформації про суміжність, та іншої детальної інформації про переадресацію пакетів і маршрутизацію для кожного однорангового вузла. Якщо кожен вихідний вузол в наскрізній мережі стає одноранговим, в спробі зробити всі вихідні вузли одним мережним рівнем за допомогою стрибка один від одного, це значно обмежує масштабованість моделі накладення VPN.

IPsec є поширеною за використанням моделлю VPN, працює в основному на мережному рівні. Застосування шифрування через IPsec запобігає розкриттю корисного навантаження дейтаграм від початку до кінця, тому дані залишаються захищеними всередині маршрутизаторів. Корисне навантаження дейтаграми включає як заголовок транспортного рівня, так і його сегменти даних, застосування шифрування на рівні IPsec, приховання додатків та даних, що використовуються. Це забезпечує значний приріст конфіденційності, але також призводить до більш неефективного використання Інтернету, оскільки алгоритми формування трафіку в маршрутизаторах критично залежать від наявності повного доступу до транспортних заголовків. Використання шифрування на рівні IPsec також означає, що кінцевим точкам не потрібно знати, чи кожна ланка, через яку проходить дейтаграма в Інтернеті застосовує шифрування; використання шифрування на цьому рівні спрощує аналіз безпеки порівняно з шифруванням, що застосовується лише на лише на рівні MAC-адресів. Як і шифрування на рівні MAC, IPsec є зручним інструментом для впровадження шифрування прозорого впровадження шифрування для захисту застарілих додатків, які в цілому ігнорували проблеми конфіденційності. Недоліком IPsec є те, що він все ще залишає дані незахищеними всередині мережі, а шкідливе програмне забезпечення іноді може зачепитися між мережею і рівнем сокетів, щоб перевіряти трафік [16].

Управління вторгненнями охоплює виявлення, запобігання та реагування на різні небезпеки. Основою для вирішення цієї проблеми є впровадження

систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS) в точках входу в хмару, та на серверах у хмарі.

IDS та IPS - це комплекс автоматизованих засобів, призначених для виявлення несанкціонованого доступу до хост-системи. Ці інструменти призначені для моніторингу мережі та активності серверів, робочих станцій, і, як правило, базуються на сигнатурах і шукають підозрілу активність, яка відповідає попередньо налаштованій сигнатурі у режимі реального часу. Якщо умова збігається з сигнатурою, інструмент системи запобігання вторгненням або блокує, або сповіщає, якщо це систем виявлення вторгнень [17].

В основному розрізняють два типи систем виявлення вторгнень. Це мережні системи виявлення вторгнень та система виявлення вторгнень на основі хоста, класифікації, в яких зроблені на основі середовища або методу вторгнення. Зазвичай розрізняють два види IDS та IPS, а саме:

- виявлення вторгнень на основі мережі системи (NIDS). NIDS може бути незалежною платформою і спрямована на виявлення вторгнень шляхом дослідження мережевого трафіку та моніторингу декількох хостів. Ці системи отримують доступ до трафіку, поводячись у вигляді паразита на мережному концентраторі, комутаторі спеціально розробленому для віддзеркалення портів. Для точності та ефективності, датчики розташовані у стратегічно обраних місцях, в межах . Ці сенсори збирають всі мережні дані та аналізують вміст пакетів;
- система виявлення вторгнень на основі хоста (HIDS).У цьому типі IDS система зазвичай містить єдиного агента, вбудованого в різноманітну систему, який виявляє вторгнення шляхом дослідження журналів, викликів зроблених системою, модифікацій файлової системи та інших станів і дій. У HIDS програмний агент може бути сенсором [18].

Традиційно ці IDS-системи максимально використовують сигнатури відомих атак для ідентифікації вхідних даних. Але через швидкий розвиток новітніх видів шкідливого програмного забезпечення, або сигнатур, які невідомі, фільтрація постійно зростаючої кількості найсучасніших видів шкідливого

програмного забезпечення стає все складніше. Це відкрило шлях для поєднання машинного навчання та додаткових заходів кібербезпеки. Для протоколів виявлення на основі машинного навчання може бути проблемою визначення класифікації атаки. Тому, для навчання моделі використовується неупереджений набір даних , при якому модель оптимізована для інтеграції в протоколи, для більш точного прогнозування шкідливого програмного забезпечення. Цей принцип прогнозування усуває повну залежність від сигнатур виявлення шкідливого програмного забезпечення, а отже, є перевагою над традиційними системами виявлення. Для того, щоб модель прогнозування працювала ефективніше, треба забезпечити її великою кількістю навчальних даних. Часто ці дані не позначені, і доступні з неправильною функціональною інженерією.

Пастка традиційного машинного навчання полягає в тому, що навчальні дані повинні бути належним чином позначені, щоб модель могла шукати закономірності, а потім надавати результати прогнозування. Але це не завжди буде можливо через великі обсяги знань. Глибоке навчання має явні переваги над традиційними алгоритмами в сценаріях обробки неструктурованих даних. Виявлення закономірностей позбавляє нас від допоміжного завдання маркування.

3.4 Транспортний захист

На транспортному рівні використовують Transport Layer Security (TLS) - це універсальний сервіс, реалізований у вигляді набору протоколів, які покладаються на TCP (рис.3.9). На цьому рівні є два варіанти реалізації. Для більшої універсальності, TLS може надаватися як частина базового набору протоколів і, таким чином, бути прозорим для додатків. Крім того, TLS може бути вбудована в окремі пакети. Наприклад, більшість браузерів оснащено TLS, а більшість веб-серверів реалізують ці протоколи.

TLS призначений для використання TCP протоколу для забезпечення надійного наскрізного захищеного сервісу. TLS - це не один протокол, а скоріше два рівні протоколів [19].

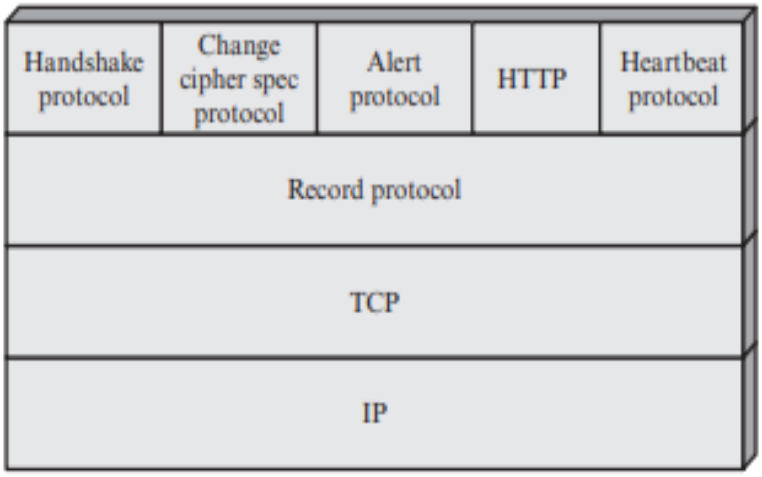

Рисунок 3.9 – Стек TLS протоколів

Протокол запису TLS надає базові послуги безпеки для різних протоколів вищих рівнів. Зокрема, протокол передачі гіпертексту (HTTP), який забезпечує передачу даних для веб-взаємодії клієнт/сервер, може працювати поверх TLS. Три протоколи вищого рівня визначені як частина TLS, а саме протокол рукостискання (Handshake), спеціальний протокол зміни шифру і протокол сповіщення. Ці специфічні для TLS протоколи використовуються для управління обміном TLS. Четвертий протокол, Heartbeat Protocol, використовується для моніторингу доступності об'єкта протоколу. Двома важливими поняттями TLS є сеанс і з'єднання TLS, які визначені в специфікації наступним чином:

- з'єднання - це своєрідний транспорт, який забезпечує відповідний тип сервісу. Для TLS такі з'єднання є одноранговими відносинами, з'єднання є тимчасовими, а кожне з'єднання асоціюється з одним сеансом;
- сеанс - TLS - це зв'язок між клієнтом і сервером. Сеанси створюються за

допомогою протоколу рукостискання. Сеанси визначають набір криптографічних параметрів безпеки, які можуть бути спільними для декількох з'єднань. Сесії використовуються, щоб уникнути дорогих переговорів про нові параметри безпеки для кожного з'єднання.

Між будь-якою парою сторін, такими як HTTP на клієнті та сервері, може існувати декілька захищених з'єднань. Між сторонами також може бути декілька одночасних сеансів. З кожним сеансом пов'язаний ряд станів. Встановлюється поточний робочий стан як для читання, так і для запису. Крім того, під час протоколу рукостискання створюються відкладені стани читання і запису створюються стани очікування для читання і запису. Після успішного завершення протоколу рукостискання стани очікування стають поточними станами.

HTTPS - це комбінація протоколів HTTP і SSL для забезпечення безпечного зв'язку між веб-браузером і веб-сервером. Її використання залежить від підтримки веб-сервером HTTPS з'єднання, бо деякі пошукові системи не підтримують HTTPS. Звичайні HTTP з'єднання використовують порт 80. При HTTPS, використовується порт 443, який викликає SSL. Коли використовується HTTPS, наступні елементи з'єднання зашифровуються:

- URL-адреса запитуваних документів;
- вміст документів;
- вміст браузерних форм (заповнених користувачем браузера);
- файли cookie, що надсилаються від браузера до сервера та від сервера до браузера;
- вміст заголовка HTTP.

Немає ніяких фундаментальних змін у використанні HTTP через SSL або TLS, і обидві реалізації називаються HTTPS.

Ініціювання з'єднання починається з того, що клієнт ініціює з'єднання з сервером на відповідному порту, а потім надсилає TLS ClientHello, щоб почати TLS-рукостискання. Коли рукостискання TLS майже завершено, клієнт може

ініціювати перший HTTP-запит. Всі дані HTTP повинні бути надсиланні як дані протоколу TLS.

Існує три рівні обізнаності про з'єднання в HTTPS. На рівні HTTP клієнт запитує з'єднання з HTTP-сервером, надсилаючи запит на з'єднання на наступний найнижчий рівень. Зазвичай наступним найнижчим рівнем є TCP, але це також може бути TLS. На рівні TLS встановлюється сеанс між TLS-клієнтом і TLS-сервером. Цей сеанс може підтримувати одне або декілька з'єднань в будь-який час. TLS-запит починається зі встановлення TCP-з'єднання між TCP-об'єктом на стороні клієнта і об'єктом TCP на стороні сервера.

На закриття з'єднання може вказати HTTP-запис, який додає HTTP-клієнт або сервер. Закриття HTTPS-з'єднання вимагає, щоб TLS закрив з'єднання з одноранговим об'єктом TLS на віддаленій стороні, що передбачає закриття базового TCP-з'єднання. На рівні TLS правильний спосіб закриття з'єднання полягає в тому, що кожна сторона використовує протокол попередження TLS.

Реалізації TLS повинні ініціювати обмін сповіщеннями про закриття. Якщо, закрити з'єднання, не чекаючи, поки однорангова програма надішле своє сповіщення, реалізація, яка робить це, може вирішити повторно використати сеанс. Це робиться лише тоді, коли програма знає, зазвичай через виявлення меж HTTP-повідомлення, що вона отримала всі дані, які його цікавлять. HTTP-клієнти також повинен бути в змозі впоратися з ситуацією, в якій основне TCP-з'єднання розривається без попереднього сповіщення і без індикатора. Така ситуація може виникнути через помилку програмування на сервері або помилкою зв'язку, яка призводить до розриву TCP-з'єднання. Однак, несподіване закриття TCP-з'єднання може свідчити про якусь атаку. Тому HTTPS-клієнт повинен видати якесь попередження про безпеку, коли це відбувається [20].

Secure Shell (SSH) - це протокол для безпечного мережного зв'язку, розроблений для того, щоб бути відносно простим і недорогим у реалізації. Початкова версія SSH-1 була зосереджена на забезпеченні захищеного віддаленого входу в систему для заміни TELNET та інших схем віддаленого входу, які не забезпечували ніякої безпеки. SSH також надає більші можливості

для архітектури клієнт/сервер і може використовуватися для таких мережних функцій, як передача файлів і електронна пошта. Нова версія SSH-2 виправляє ряд недоліків безпеки в оригінальній схемі. Клієнтські та серверні програми SSH широко доступні для більшості операційних систем. Він став методом вибору для віддаленого входу в систему, тунелювання, і швидко стає одним з найпоширеніших застосувань технології шифрування за межами вбудованих систем [21].

SSH організовано у вигляді трьох протоколів (рис. 3.10), які зазвичай працюють поверх TCP [21].

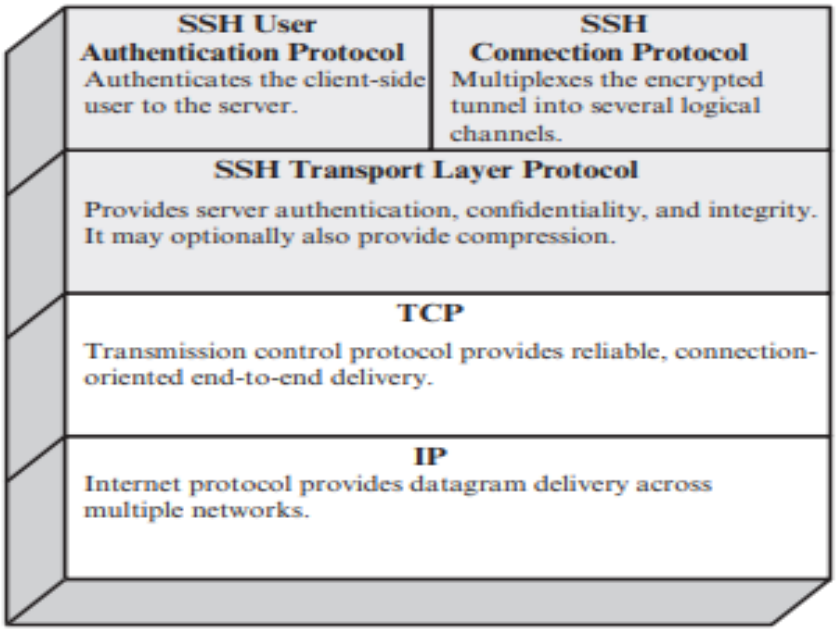

Рисунок 3.10 – Стек SSH протоколів

Протокол транспортного рівня: забезпечує автентифікацію сервера, конфіденційність даних, і цілісність даних з прямою секретністю (тобто, якщо ключ скомпрометований протягом одного сеансу, це не впливає на безпеку попередніх сеансів). Транспортний рівень може додатково забезпечувати стиснення.

Протокол автентифікації користувача: автентифікує користувача на сервері.

Протокол з'єднання: мультиплексує декілька логічних каналів зв'язку через одне, базове SSH-з'єднання.

3.5 Хмарний захист

Хмарний захист складається з управління ідентифікацією та розподілення доступу, оцінки безпеки, комплексу захисту “Web security”, агрегатів інформації про безпеку та управління подіями, а також запобігання втрати даних. Ці складові може надавати провайдер хмарних сервісів (CSP), який і надає хмару для користування (рис. 3.11). Однак, в залежності від провайдеру, деякі з цих складових можуть бути опціональними [22].

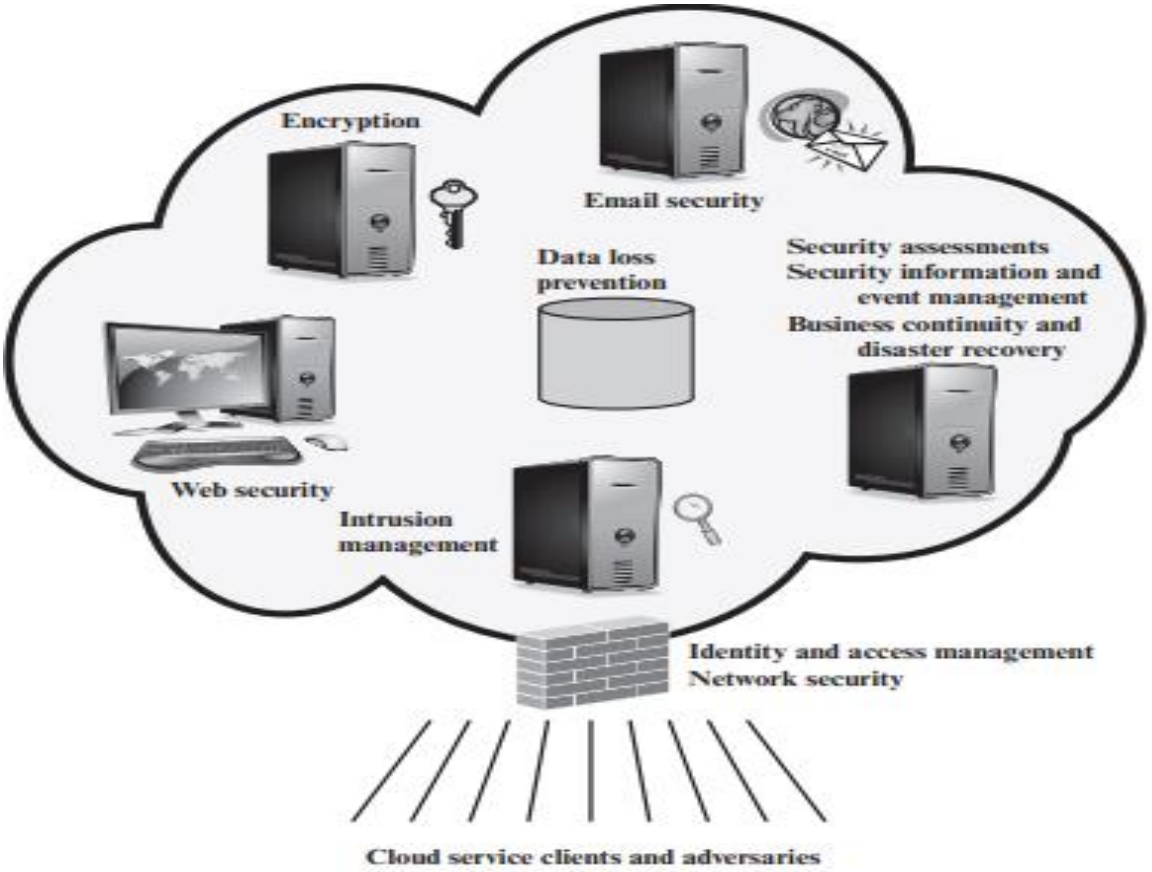

Рисунок 3.11 – Елементи послуг хмарного захисту

Управління ідентифікацією та доступом (IAM) включає в себе процеси та системи, які використовуються для управління доступом до ресурсів підприємства шляхом забезпечення того, що визначає ідентичність суб'єкта, а потім надає правильний рівень доступу на основі цієї підтвердженої ідентичності. Одним з аспектів управління ідентифікацією є надання ідентифікаційних даних, що пов'язано з наданням доступу ідентифікованим користувачам, або відмовою в доступі і подальшим позбавленням доступу, коли підприємство-клієнт визначає таких користувачів як таких, що більше не мають доступу до корпоративних ресурсів у хмарі. Інший аспект управління ідентифікацією це є участь хмари у федеративній схемі управління ідентифікацією ідентичностями, що використовується підприємством-клієнтом. Частина IAM, що стосується управління доступом, включає в себе автентифікацію та управління доступом. Наприклад, CSP повинен мати можливість автентифікувати користувачів. Вимоги до контроля доступу в середовищах SPI включають створення надійного профілю користувача та інформації про політику, використання її для доступа в хмарному сервісі, і робити це так, щоб це можна було перевірити.

Запобігання втраті даних (DLP) - це моніторинг, захист і перевірка безпеки даних у стані спокою, в русі та під час використання. Значна частина DLP може бути реалізована хмарним клієнтом. CSP також може надавати послуги DLP, такі як впровадження правил щодо того, які функції можна виконувати над даними у різних контекстах.

Web Security - це захист у реальному часі, який пропонується або на місці за допомогою встановлення програмного забезпечення (пристрою), або через хмару шляхом проксі-сервера чи перенаправлення веб-трафіку на ЦП. Це забезпечує додатковий рівень захисту на додаток до таких засобів, як антивіруси, щоб запобігти проникненню шкідливого програмного забезпечення на підприємство через такі дії, як перегляд веб-сторінок. На додаток до захисту від шкідливого програмного забезпечення, хмарна служба веб-безпеки може

включати дотримання політики використання, резервне копіювання даних, контроль трафіку та контроль веб-доступу. CSP може надавати послугу електронної пошти, для якої необхідні заходи безпеки. Безпека електронної пошти забезпечує контроль над вхідною та вихідною електронною поштою, захищає організацію від фішингу, шкідливих вкладень, забезпечує дотримання корпоративних політики, такі як прийнятне використання та запобігання спаму. CSP може також включати цифровий підпис на всіх поштових клієнтах і забезпечувати додаткове шифрування електронної пошти.

Безперервність бізнесу та аварійне відновлення включають в себе заходи та механізми для забезпечення операційної стійкості в разі будь-яких перебоїв у наданні послуг. Це сфера, де CSP, завдяки економії на масштабах, може запропонувати очевидні переваги клієнту хмарного сервісу. CSP може забезпечити резервне копіювання в декількох місцях, з надійними засобами обходу відмов та аварійного відновлення. Ця послуга повинна включати гнучку інфраструктуру, резервування функцій та обладнання, контрольовані операцій, географічно розподілені центри обробки даних та відмовостійкість мережі.

Агрегати інформації про безпеку та управління подіями (SIEM) - збирають данні журналів і подій з віртуальних і реальних мереж, додатків і систем. Потім ця інформація співвідноситься і аналізується, щоб забезпечити в реальному часі звітності та оповіщення про інформацію/події, які можуть вимагати втручання або іншого типу реагування. CSP зазвичай надає інтегровану послугу, яка може об'єднати інформацію з різних джерел як у хмарі, так і в корпоративній мережі клієнта, як у хмарі, так і в корпоративній мережі клієнта.

Оцінка безпеки – можна частово додати до хмарного захисту, це аудит хмарних сервісів третьою стороною. Хоча ця послуга знаходиться за межами компетенції CSP, CSP може надавати інструменти та точки доступу для полегшити проведення різних заходів з оцінювання.

3.6 Апаратний захист

Апаратний захист вважається та розглядається як залежна і надійна частина системи захисту мереж, тому і слід враховувати і не ігнорувати цей аспект захисту. Зловмисники зазвичай можуть мати фізичний доступ до апаратних компонентів системи і можуть використовувати розширений аналіз побічних каналів для отримання захищеної інформації, що надійно зберігається в системі. Вони також можуть спричинити фізичні збурення в системі, наприклад, застосовуючи сильні електромагнітні імпульси, щоб маніпулювати її роботою, та перестрибнути перевірку пароля [23].

До апаратного забезпечення відносяться компоненти мережної платформи, такі як, ноутбук, портативний комп’ютер, комутатор, маршрутизатор, бездротову точку доступу або кабелі, які використовуються для підключення пристроїв. Іноді деякі компоненти мережі можуть бути невидимими, у випадку бездротових медіа, де повідомлення передаються через повітря за допомогою радіочастот або інфрачервоних хвиль.

До деяких типів апаратного захисту відносяться:

- біометричні системи доступу;
- системи контролю доступу.

Біометричні системи дозволяють визначати особу на основі унікальних фізіологічних характеристик, використовуючи технічні засоби для забезпечення надійності та швидкості обробки даних. Сканери відбитків пальців використовують оптичні чи капацитивні технології для створення унікального "відбитку" пальця та порівняння його з зареєстрованими шаблонами. Оптичні сканери використовують світлові сенсори для отримання відображення відбитків пальців, а капацитивні сканери вимірюють зміну ємності при доторканні пальця, створюючи 3D-зображення.

Системи розпізнавання обличчя використовують алгоритми глибинного навчання для аналізу ключових точок та унікальних рис обличчя для ідентифікації особи. А також використовують нейронні мережі для виявлення та

аналізу ключових особливостей обличчя, аналіз геометричних параметрів, таких як відстань між очима та форма обличчя.

Сканери ретини визначають особу за унікальними характеристиками судин на задній частині очей, забезпечуючи високий рівень надійності. Застосовують інфрачервоне світло для створення високороздільних зображень судин.

Для додаткового технічного захисту біометричних систем застосовують шифрування даних біометричних характеристик, анти-спуфінг- виявлення тепла чи живої тканини, для уникнення атак, спрямованих на підміну біометричних даних, а також, в деяких випадках, двофакторну автентифікацію.

Системи контролю доступу використовують різноманітні технічні рішення для ефективного та безпечного обмеження фізичного доступу, наприклад, застосування електронних замків та кард-рідерів на основі RFID технології.

Електронні замки використовуються для автоматизованого управління фізичними бар'єрами. Їх використовують як механізми блокування у випадках екстрених ситуацій.

Кард-рідери та RFID технології можуть використовувати картки або брелоки з RFID чипами для безконтактної автентифікації, припускають використання радіочастоти та чипів для безконтактного обміну даними між карткою та читачем, застосовуються алгоритми шифрування для захисту від зламу та клонування.

4 РОЗРОБКА ІНФОРМАЦІЙНОГО ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1 Розробка системи захисту на основі виділиних технологій та ресурсів

У майбутньому всі джерела даних і обчислювальні сервіси будуть розглядатися як ресурси, в яких весь доступ буде динамічним і строго регламентованим. Традиційні підходи до забезпечення безпеки на основі периметра вже не є достатньо безпечними через те, що, якщо пристрій скомпрометовано, зловмисник може отримати доступ до всіх ресурсів не проходячи через периметр. На відміну від підходів до безпеки на основі периметра, модель безпеки з нульовою довірою (Zero Trust) дотримується принципу "перевіряй і ніколи не довіряй" і припускає, що будь-який доступ до системи є ненадійним і потребує перевірки, та спрямований на покращення безпеки в умовах розподіленого доступу до ресурсів, і є перспективним підходом. До основних елементів захисту мережі на основі Zero Trust можна віднести:

- мікроперіметри та сегментацію мережі, де мережа розділяється на невеликі мікроперіметри та встановлюється обмежений контроль доступу між ними, на основі цієї інформації формуються жорсткі правила доступу;
- ідентифікацію, аутентифікацію та авторизацію; для встановлення персони, наданою нею інформації (пароля тощо) та її рівня допуску;
- моніторинг та аналітику підозрілої активності користувачів, трафіку, пристроїв, подій, на виявлення аномалій;
- додаткове шифрування даних;
- технології навчання штучного інтелекту, чи просто машиного алгоритмум для виявлення заагроз та вдосконалення систем безпеки на основі вивчення здобутого досвіду [24].

За основу розробки корпоративної мережі був обраний офіс «Кімерія» (довільна назва офісу), який знаходиться на 4-ому поверсі будівлі. З технічних

пристроїв нам доступно 17 робочих станцій (1 на пункті контролю), 1 серверний термінал, та 4 серверні шафи. Графічне зображення обладненого офісу знаходиться на рис. 4.1.

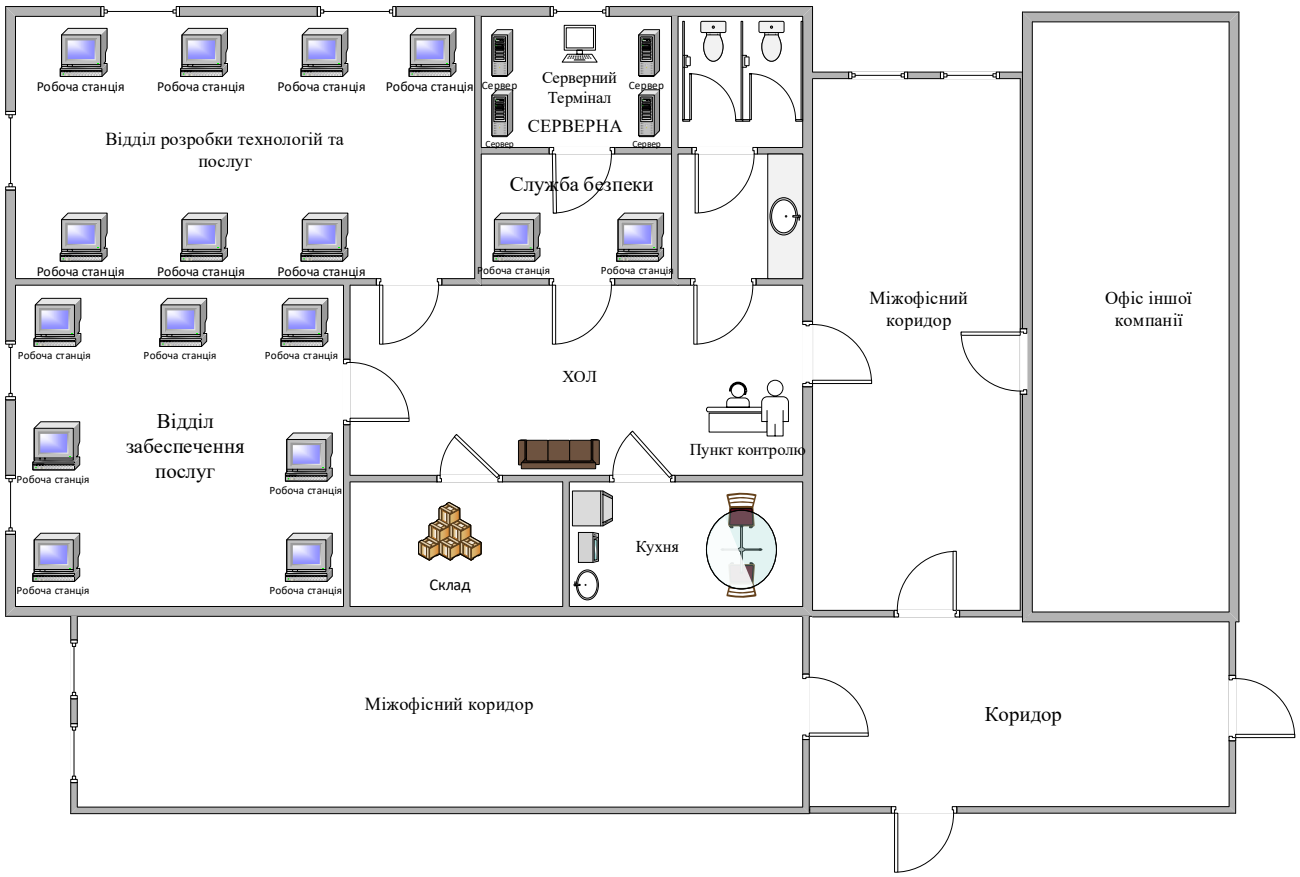

Рисунок 4.1 – Загальна схема офісу корпоративної мережі

Мережа будується на основі моделі безпеки Zero Trust, тому треба врахувати, де знаходяться канали витоку інформації, зони комерційної таємниці, та, на основі цієї інформації, належним чином використати засоби захисту від втрати даних.

До каналів витоку інформації можна віднести:

- візуальне знімання з пристроїв (фото, відео);
- пристрій для прослуховування в стінах та меблях;
- внутрішній канал витоку через персонал (вербальний);
- здобуток інформації за допомогою соціальної інженерії;

- здобуток акустичної інформації з використанням диктофонів;
- крадіжка носіїв інформації;
- лазерне знімання акустичної інформації з вікон;
- несанкціоноване копіювання;
- витік за рахунок несправності протоколів захисту;
- витік каналами зв’язку (телефон тощо);
- витік через шкідливе програмне забезпечення.

Можна ще багато додати до каналів витоків інформації, однак зосередимося тільки на захисті від прямих фізичних витоків (скачування, крадіжка носіїв, тощо), та від логічніх витоків. На рис. 4.2 зображені зони комерійної інформації та привентивні системи захисту.

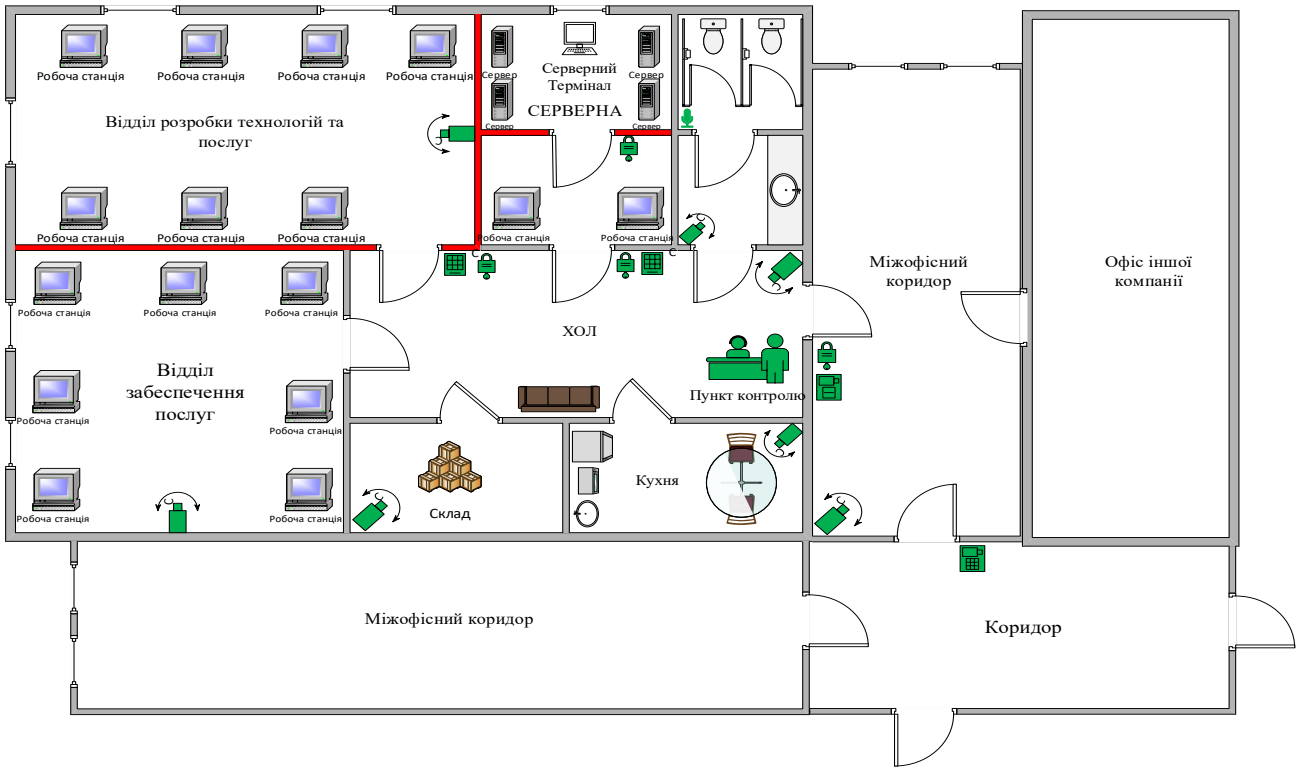

Рисунок 4.2 – Зона комерційної таємниці та засоби захисту від втрати даних методом фізичної взаємодії

До привентивної системи захисту від фізичних витоків відносяться 7 панорамних камер з вбудованими мікрофонами, 1 мікрофон у вбиральні, який виконує функції виявлення несанкціонованих розмов, 2 панелі доступу на електроному замку, котрі відрізняються рівнем доступу в залежності від посади працівника, також, 2 панелі доступу з камерами, які контролюються з пункту контролю та виконують функції захисту від вторгнення та взлому до офісу. Механічні замки у кількості 4-ох штук виконують фунцію додаткового захисту у нічний час.

Активними системами захисту від фізичних та, частково, логічних витоків вважаються два працівники служби безпеки, вони мають найвищий рівень допуску. Функціями служби безпеки є аналіз мережі на знаходження аномального трафіку, введення запобіжних дій при загрозах на мережу, відслідковування працівників на зловмисні дії та переодичний огляд. Частково до активного захисту можна приписати і співробітника пункту контролю. Він виконує банальну фільтрацію відвідувачів (відкриває чи закриває двері), та виконує функції відділу забезпечення послугами. Цей співробітник не має високого рівня доступу, як у служби безпеки.

Корпоративна мережа офісу «Кімерія» була збудована на основі моделі захисту ZeroTrust, тому для відповідності до моделі було використано мережу VLAN на основі топології «Зірка». Зображення схеми локальної мережі на рис. 4.3. Для реалізації мережі було виділено оптоволоконний кабель; 3 комутатори ; 1 двоканальний комутатор, або комутатор з фукцією Frame Switching, який виконує функції розділення мережі на дві підмережі за допомогою аналізування MAC-адреси в мережних пакетах і направляє їх лише на порт, до якого підключений пристрій з відповідною адресою для забезпечення ізольованості трафіку однієї групи від іншої; 1 маршрутизатор в серверній кімнаті, котрий з’єднує мережі для завантаження всієї інформаціїї на сервера, а також 1 WI-FI – маршутизатор біля виходу з офісу, який виконує функції захисту, фільтрації та відокремлення трафіку локальної мережі від глобальної і забезпечує персонал та випадкових відвідувачей обмеженим політиками захисту доступом до інтернету.

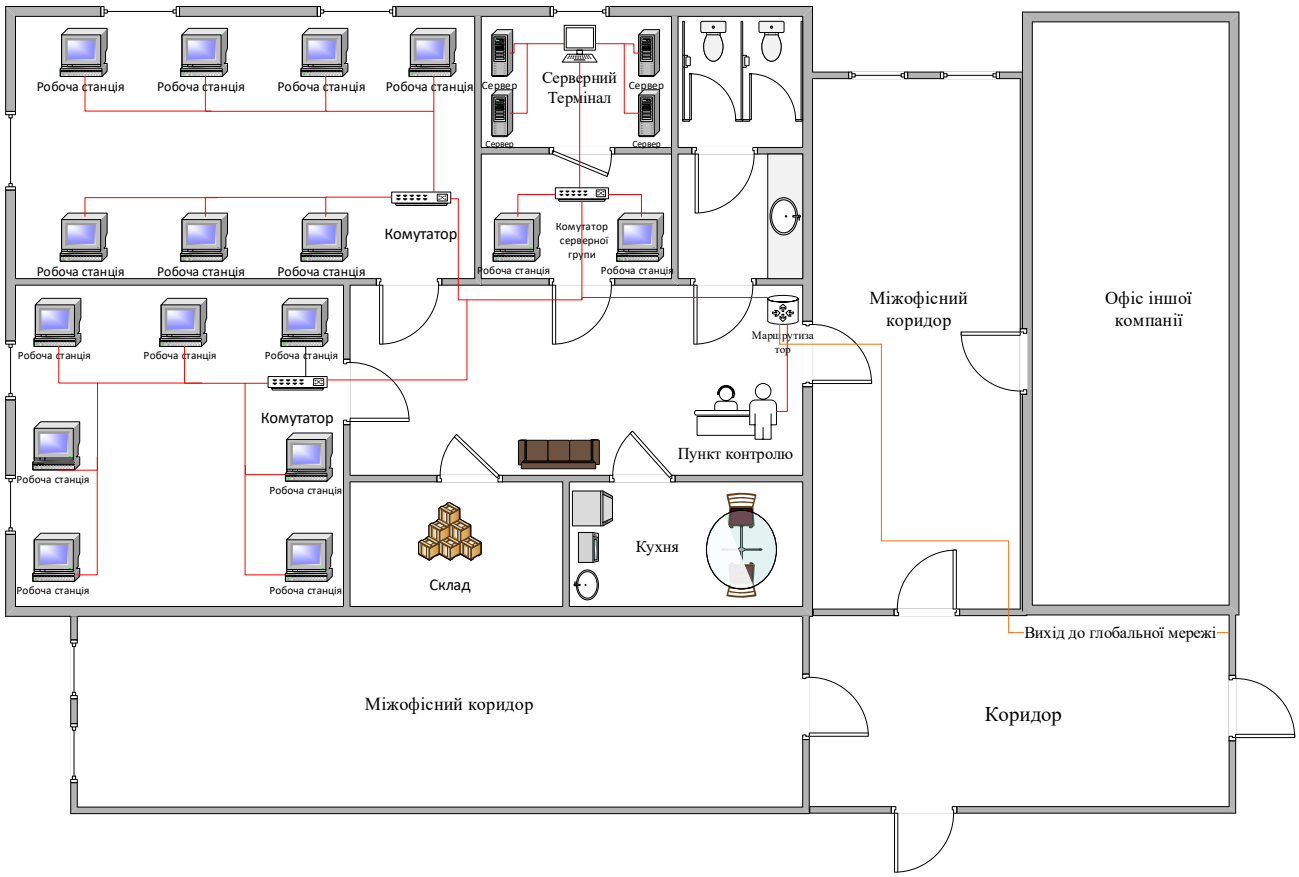

Рисунок 4.3 – Схема корпоративної локальної мережі VLAN на основі топології «зірка»

4.2 Налаштування системи захисту та обладнання

Для захисту логічної структури системи можна застосувати багато засобів захисту інформації, однак для опису та реалізації були взяті приклади роботи та налаштування VLAN, а також маршрутизатора. За основу побудови мережі, в якій буде йти розробка, взято програмне забезпечення Cisco Paket Tracer (рис. 4.4). Метою використання цієї програми є побудова прообразу мережі, симуляція та перевірка системи на стабільну роботу. Але основним завданням є відтворення алгоритму побудови віртуальної мережі, а також прив’язка їх до інтерфейсів комутатора на основі програмного забезпечення.

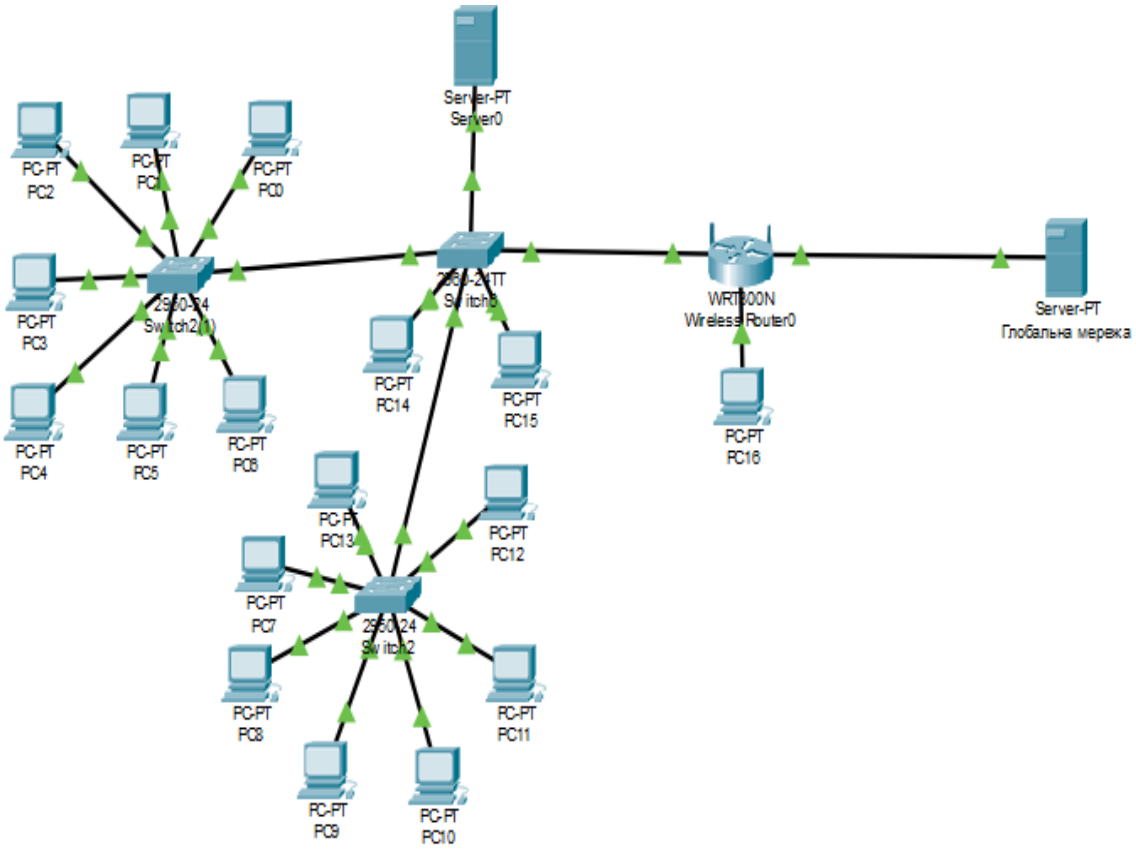

Рисунок 4.4 – Схема мережі у Cisco Paket Tracer

Для початку зробимо під’єднання адміністративного ком’ютера до серверного комутатора за допомогою протоколу SSH. Почнемо з того, що вимкнемо відповідь DNS-запитів, це зроблено для того, щоб при введені команди неправильно, обладнання не інтерпретувало її як доменне ім'я та не намагалося вирішити його через службу DNS. Наступним кроком була змінена назва пристрою, задано доменне ім’я, логін користувача та пароль. Для більшої безпеки втановили другу версію SSH та увімкнули генерування RSA-ключа, де наш ключ має розмір 512 біт. У режимі конфігурації вказали на те, щоб лінії віртуального терміналу використовували тільки протоколи SSH. Після, створили ВЛАН №19 під назвою «sysadm» та задали для нього IP: 192.168.99.28, маску: 255.255.255.0, і зберегли конфігурацію. На рис. 4.5 зображені основні налаштування серверного комутатора.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname sw-arm
sw-arm(config)#ip domain name admin
sw-arm(config)#username admin password 12345
sw-arm(config)#enable password 12345
sw-arm(config)#ip ssh version 2
Please create RSA keys (of at least 768 bits size) to enable SSH v2.
sw-arm(config)#crypto key generate rsa
The name for the keys will be: sw-arm.admin
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

sw-arm(config)#line vty 0 4
*Бер 1 0:2:34.355: RSA key size needs to be at least 768 bits for ssh version 2
*Бер 1 0:2:34.355: %SSH-5-ENABLED: SSH 1.5 has been enabled
sw-arm(config-line)#transport input ssh
sw-arm(config-line)#login local
sw-arm(config-line)#vlan 19
sw-arm(config-vlan)#name contrl
sw-arm(config-vlan)#int vlan 19
sw-arm(config-if)#
%LINK-5-CHANGED: Interface Vlan19, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan19, changed state to up

sw-arm(config-if)#ip address 192.168.99.28 255.255.255.0
sw-arm(config-if)#no sh
sw-arm(config-if)#exit
sw-arm(config)#do wr
```

Рисунок 4.5 – Основні налаштування серверного комутатора

Для подальших дій треба провести транкування інтерфейсів комутатора. Цей процес дозволяє передавати дані VLAN через одне фізичне обладнання. Налаштування проводиться у режимі конфігурації, де вказується інтерфейс який повинен бути транковим. Далі прописується сам процес транкування, після якого можна вважати, що комутатор вже є транком. Додаткові комутатори теж треба робити транковими, наприклад комутатор групи розробки. Рис. 4.6 та 4.7 зображають процеси транкування комутаторів.

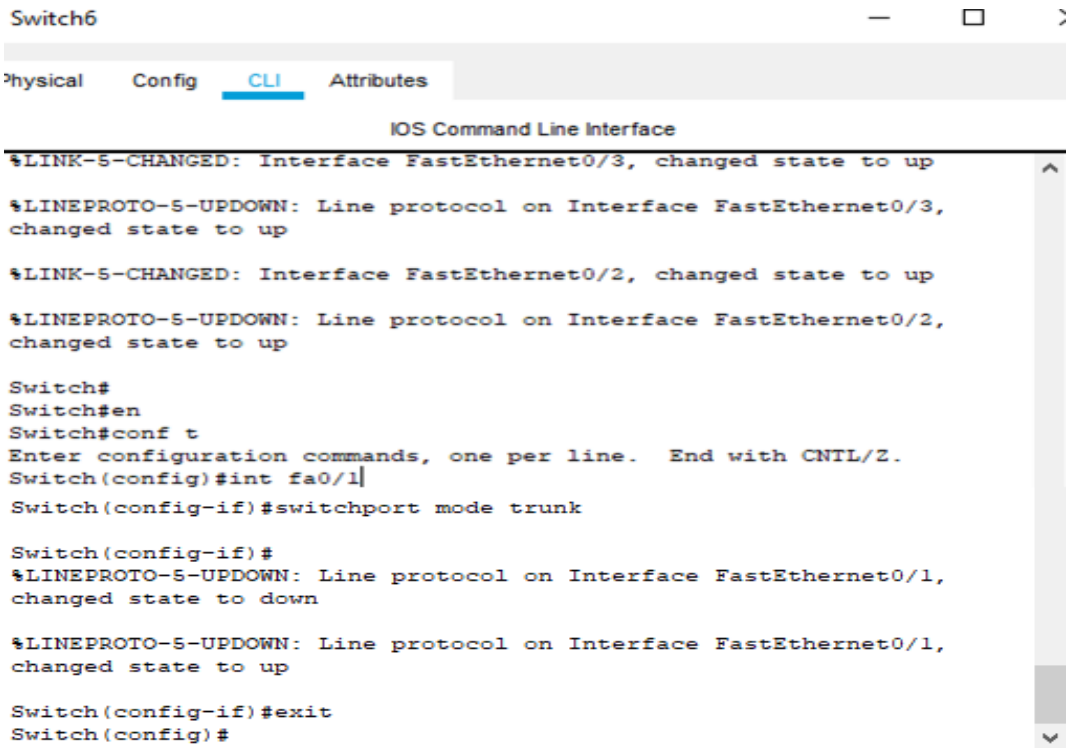

Рисунок 4.6 – Транкування інтерфейсу серверної групи

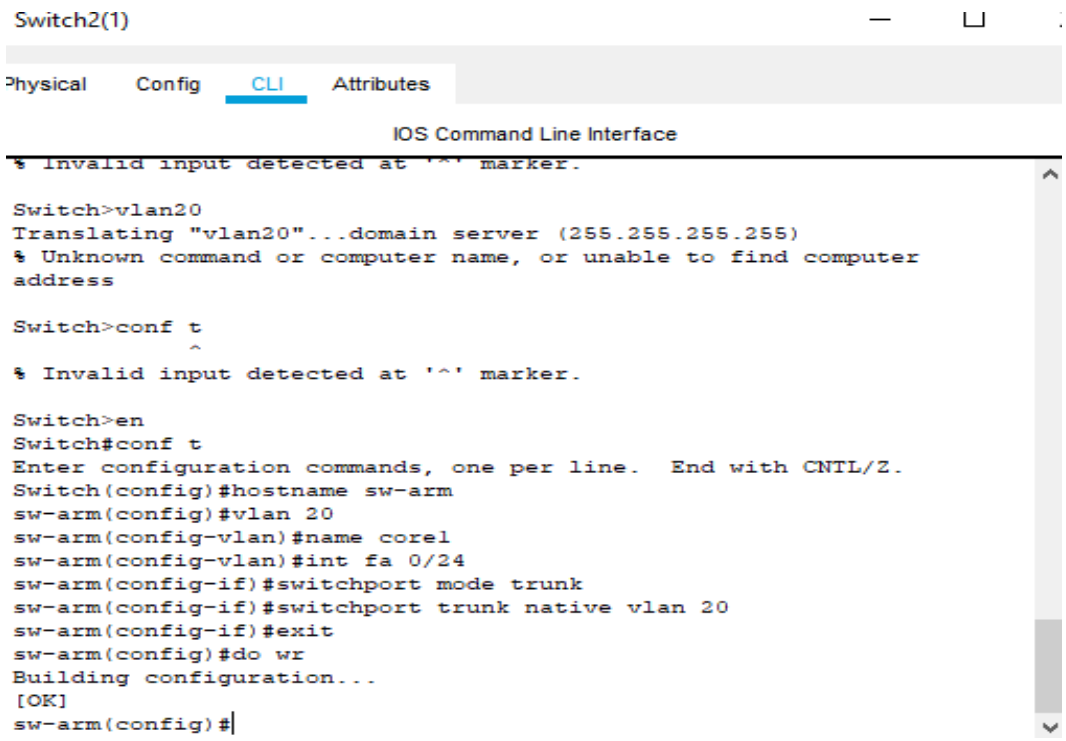

Рисунок 4.7 – Транкування комутатора групи розробки

Режим доступу (Access mode) використовується для під’єднання кінцевих робочих станцій (комп’ютерів, принтерів тощо). Рис. 4.8 наглядно показує принцип під’єднання робочої станції до комутатора. У режимі конфігурації спочатку прописуються діапазон інтерфейсів, котрі треба використовувати. Можна прописати і один інтерфейс. Також прописується призначення номерів віртуальної мережі для сортування трафіку.

```
sw-arm(config)#vlan 13
sw-arm(config-vlan)#name inv
sw-arm(config-vlan)#int range 0/1-5
                      ^
% Invalid input detected at '^' marker.

sw-arm(config-vlan)#int range fa0/1-5
sw-arm(config-if-range)#switchport mode access
sw-arm(config-if-range)#switchport access vlan 12
sw-arm(config-if-range)#exit
sw-arm(config)#do wr
Building configuration...
[OK]
sw-arm(config)#
```

Рисунок 4.8 – Створення групи VLAN, призначення веб-інтерфейсів до нього, включення коммутаторів до access mode

Налаштування бездротового маршрутизатора є одним із важливих аспектів забезпечення та захисту мережі. Для початку роботи обрано статичну IP-адресу 10.99.0.2 та маску 255.255.255.248 (рис. 4.9). Шлюзом для пристрою буде IP-адреса інтерфейу fastethernet 0/0, який був вказаний у комутаторі серверної групи. На рис. 4.10 зображено наступний етап налаштування, де номера IP-адреса призначаються співробітникам чи клієнтам. Усього доступно 29 хостів для під’єднання. Також вказується адреса DNS серверу, для під’єднання почтового серверу до мережі.

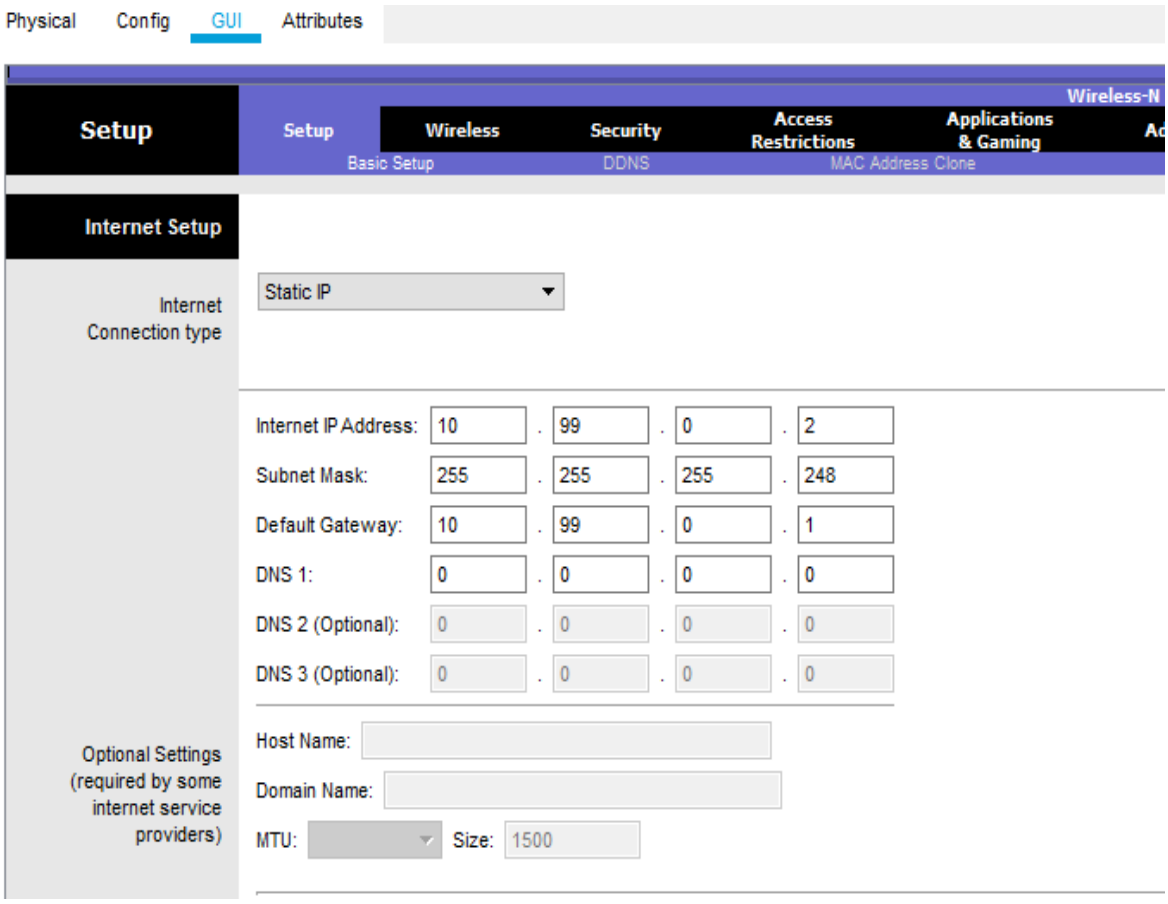

Рисунок 4.9 - налаштування IP-адресу, маски, та шлюзу

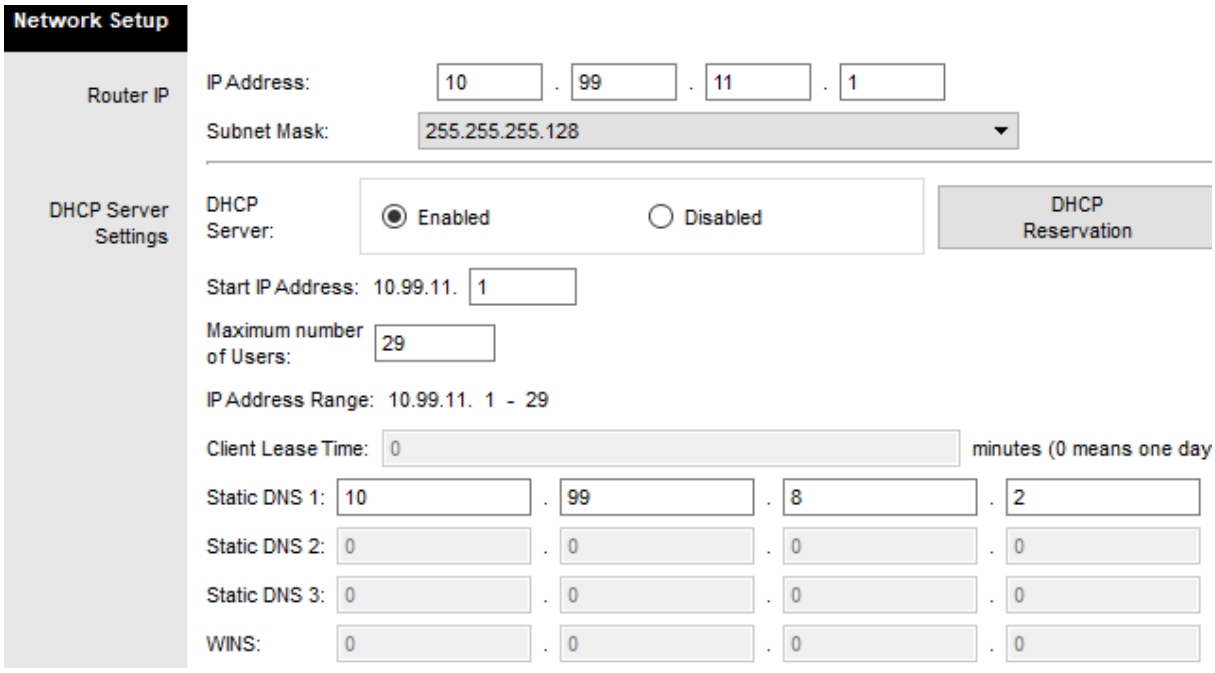

Рисунок 4.10 – налаштування роздачі IP-адресу персоналу

Наступним етапом є створення назви «corp guest» у вкладці basic wireless settings (рис. 4.11). Тут також можна змінити деякі параметри, наприклад для створення ширококанальної мережі. Однак вирішено все залишити у стандартному налаштуванні. Для встановлння протоколу безпеки та паролю мережі перейшли на вкладку wireless security (рис. 4.12), з наданих протоколів було обрано WPA2 на основі алгоритму шифрування AES.

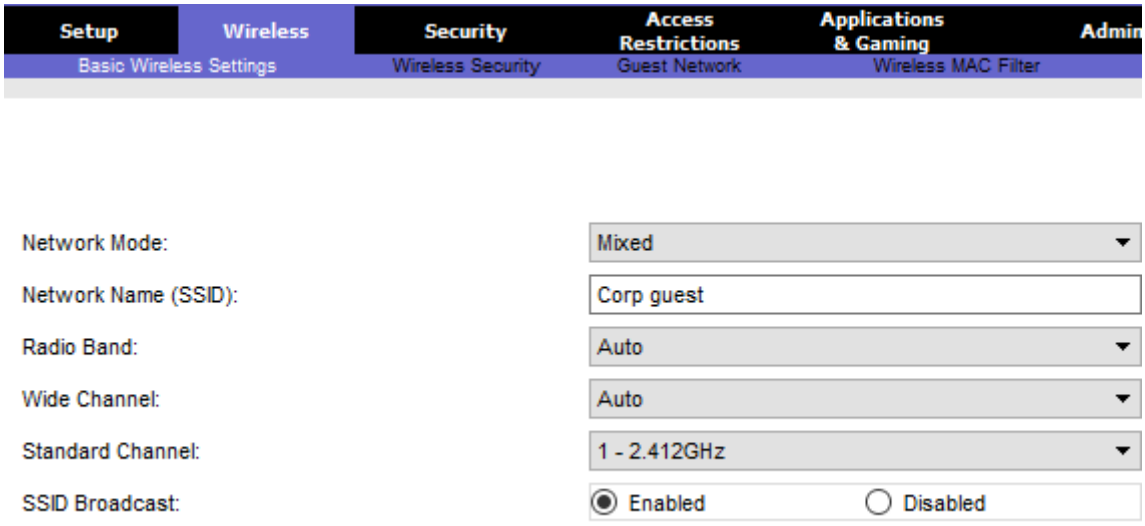

Рисунок 4.11 – Базові налаштування маршрутизатора

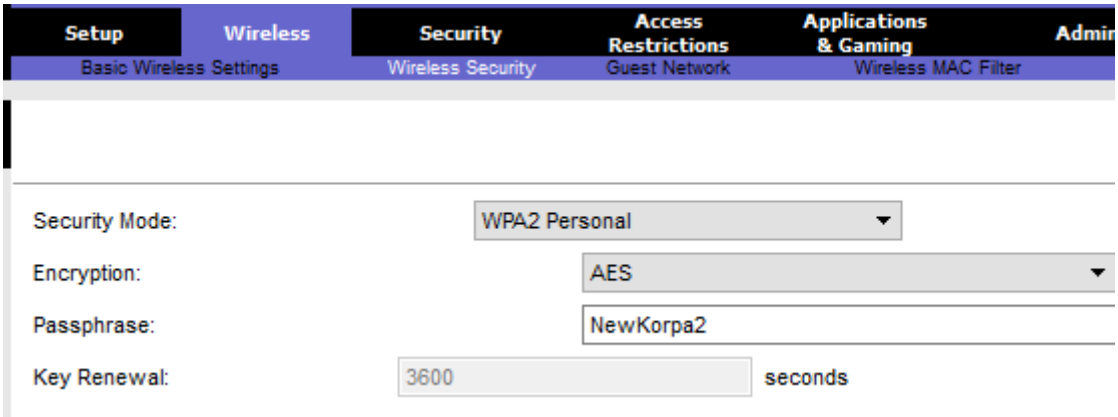

Рисунок 4.12 – Налаштуавння безпеки шляхом вибору протоколу безпеки, шифрування та встановлення паролю

ВИСНОВКИ

У ході виконання кваліфікаційної роботи магістра було проаналізовано питання технологій захисту та розроблено шляхи захисту корпоративних мереж від потенційних загроз втрати інформації. У зв’язку з ростом кількості інформації, розробка системи захисту корпоративної мережі стає невід’ємною складовою для забезпечення цілісності інформації.

Під час написання атестаційної роботи було:

- проаналізовано багато статей, матеріалів, навчальної та науково-технічної літератури;
- вивчено та представлено структуру та типи сучасних корпоративних мереж;
- досліджено потенційні ризики та наслідки загроз, поняття та види DDoS – атак;
- розглянуто різні типи засобів інформаційного захисту, таких як криптографічний, мережний, транспортний, хмарний та апаратний;
- розроблено системи захисту на основі виділеної корпоративної мережі, виконані відповідні налаштування системи VLAN та мережного маршрутизатору.

При цьому можна зробити наступні висновки.

1) Питання захисту інформації завжди буде актуальним, так як існує багато видів загроз на втрату інформації. Для цього потрібно знати методи виявлення та захисту від них.

2) Організація безпеки даних корпоративних мереж полягає не тільки в виявленні, систематизації і відображенні загроз, а головне – в управлінні ризиками, вчасні і правильні дії для зниження ризику загроз, щоденна робота по системному забезпеченню безпеки. Щоб вирішити данну проблему вже недостатньо виявляти і реагувати на дії порушників. Потрібно знаходити і виключати уразливі місця системи.

Отже, завдання кваліфікаційної роботи виконані. Отримані знання та інформація надалі можуть бути використані для розробки системи інформаційного захисту, тому що це є постійним процесом, який вимагає від співробітників організацій високого рівня обізнаності та готовності до невпинного удосконалення, з метою забезпечення ефективного захисту цінної інформації та забезпечення безпеки мережних інфраструктур, систем, незалежно від масштабу, територіального розміщення чи призначення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Stallings W. Network Security Essentials Applications and Standards / William Stallings // Network Security Essentials Applications and Standards / William Stallings. – Harlow: Pearson Education Limited, 2017. – (Pearson Education Limited). – (6). – С. 164–165.

2. Bonaventure O. Computer Networking : Principles, Protocols and Practice / Olivier Bonaventure. – Washington: The Saylor Foundation, 2011. – 5-6 с. – (The Saylor Foundation).

3. Bonaventure O. Computer Networking : Principles, Protocols and Practice / Olivier Bonaventure. – Washington: The Saylor Foundation, 2011. – 240 -241с. – (The Saylor Foundation).

4. Idika N. Proactive Detection of Computer worms / N. Idika, P. Mathur. – Purdue: Purdue University, 2007. – 48 с. – Volume 3.

5. Koret J. The antivirus hacker’s handbook / J. Koret, P. Bachaalany // The antivirus hacker’s handbook / J. Koret, P. Bachaalany. – Indianapolis: John Wiley & Sons Inc, 2015. – (John Wiley & Sons Inc). – С. 13–15.

6. Elisan C. Malaware, Rootkits & Botnets. A beginner guide. / Elisan // Malaware, Rootkits & Botnets. A beginner guide. / Elisan. – Huston: McGraw Hill Professional, 2012. – (McGraw Hill Professional). – С. 11.

7. Thomas F. Adware: The Only Book You`ll ever need / Thomas // Adware: The Only Book You`ll ever need / Thomas., 2015. – (Lulu Press). – С. 3–4.

8. Skoudis E. Malware: Fighting malicious code / E. Skoudis, L. Zeltser // Malware: Fighting malicious code / E. Skoudis, L. Zeltser., 2004. – (Prentice Hall Professional). – С. 7.

9. Singh K. Performance analysis of agent based distributed defense mechanisms against ddos attacks / Singh K, Singh Dhindsa K, Bhushan B. // International journal of computing. – 2018. – С. 15–24.

10. Zargar S. A survey of defense mechanisms against distributed denial of service

(ddos) flooding attacks / Zargar S, Joshi J, Tipper D. – 2013. – C. . 2046–2069.

11. Stallings W. Network Security Essentials Applications and Standards / Stallings // Network Security Essentials Applications and Standards / Stallings. – Harlow: Pearson Education Limited, 2017. – (Pearson Education Limited). – (6). – C. 52–54, 55-59.

12.Tanenbaum A. Computer Networks / A. Tanenbaum, D. Wetheral // Computer Networks / A. Tanenbaum, D. Wetheral. – Amsterdam: Pearson Education Limited, 2018. – (Pearson Education Limited). – (5). – C. 818–821.

13. Vidthya R. Paper on Types of Firewall and Design Principles / R. Vidthya, C. Shahu, K. Kamalesh. // International Journal of Science and Research. – 2016. – №5. – C. 1583–1584.

14. Stallings W. Network Security Essentials Applications and Standards / Stallings // Network Security Essentials Applications and Standards / Stallings. – Harlow: Pearson Education Limited, 2017. – (Pearson Education Limited). – (6). – C. 417-420.

15. Ferguson P. What is a VPN? / P. Ferguson, G. Huston. // Lulu Press. – 2007. – №1. – C. 1–3.

16. Vacca J. Computer and Information Security Handbook / John Vacca // Computer and Information Security Handbook / John Vacca. – Waltham: Morgan Kaufmann Publishers, 2013. – (2). – C. 212–213.

17. Agrawal S. Intrusion Detection System / S. Agrawal, P. Walke, S. Pandit. // International Journal of Scientific Research in Science. – 2020. – C. 1–4.

18. Vanishree K. INTRUSION DETECTION SYSTEM / Vanishree. // College of Engineering Bangalore. – 2020. – C. 2–4.

19. Comer D. Internetworking With TCP/IP / Comer // Internetworking With TCP/IP / Comer. – Columbus: Pearson Education Limited, 2014. – (Pearson). – (1). – C. 51-53.

20. Pedersen T. HTTPS, Secure HTTPS / Torben Pedersen // Encyclopedia of Cryptography and Security / Torben Pedersen. – Eindhoven: Eindhoven University of Technology, 2005. – (Eindhoven University of Technology). – C. 268–269.

21.Stallings W. Network Security Essentials Applications and Standards / Stallings // Network Security Essentials Applications and Standards / Stallings. – Harlow: Pearson Education Limited, 2017. – (Pearson Education Limited). – (6). – C. 208-215.

22. Death D. Information Security Handbook / Darren Death // Information Security Handbook / Darren Death. – Birmingham: Packt Publishing, 2017. – (Birmingham). – C. 262–268.

23. Schou C. Information Assurance Handbook / C. Schou, S. Hernandez // Information Assurance Handbook / C. Schou, S. Hernandez., 2015. – (McGraw-Hill Education). – C. 190–191.

24. Shan L. Future Industry Internet of Things with Zero-trust Security / L. Shan, I. Muddesar, S. Neetesh. // Information Systems Frontiers. – 2021. – C. 4–6.