НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри

Комп'ютерних систем, мереж та кібербезпеки

_____ Касаткін Д.Ю., к. пед.н., доц.

підпис ПІБ, вчене звання і ступінь

«___»_____ 2025 р.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

На тему: «Адмінустрування захищеними системами у корпоративній мережі»

Спеціальність F7 «Комп’ютерна інженерія»

Гарант освітньої програми: _____ / Нікітенко Є.В. /

підпис ПІБ

Керівник дипломного проекту: _____ / Мамченко С.М. /

підпис ПІБ

Виконав: _____ /Лейко Я.О. /

підпис ПІБ

КИЇВ-2025

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки

_____/ Касаткін Д.Ю., к.пед.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 2025 р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ СТУДЕНТУ

Лейко Ярослав Олегович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): F7 Комп'ютерна інженерія
Тема кваліфікаційної бакалаврської роботи: «Адміністрування захищеними системами у корпоративній мережі»
затверджена наказом ректора НУБіП України від "_16_" _12___ 2024р. №2251«С»
Термін подання завершеної роботи на кафедру _28.05.2025 року____
Вихідні дані до кваліфікаційної бакалаврської роботи Проектування та розробка захищеної системи у корпоративній мережі

Перелік питань, що підлягають розробці:
1. Аналіз технічного завдання
2. Аналіз сучасних засобів захисту мережі
3. Розробка захищеної мережі

Перелік графічного матеріалу (за потреби) презентація, рисунки, таблиці

Дата видачі завдання "_16_**"** ____12__ ____2024 р.

Керівник бакалаврської роботи _____ Мамченко С.М., д.пед.н., професор
(підпис) (прізвище та ініціали)
Завдання прийняв до виконання _____ _Лейко Я.О._____
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз предметної області	04.02.2025 р.	Виконано
2	Проектування системи	15.03.2025 р.	Виконано
3	Реалізація системи	10.04.2025 р.	Виконано
4	Тестування системи	01.05.2025 р.	Виконано
5	Оформлення пояснювальної записки	21.05.2025 р.	Виконано
6	Оформлення графічного матеріалу	25.05.2025 р.	Виконано

Студент _____ Ярослав ЛЕЙКО

(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ Сергій МАМЧЕНКО

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 65 сторінок, 39 рисунків, 3 таблиці, 13 джерел.

Об’єкт аналізу – процес адміністрування захищених систем у корпоративній мережі, що включає організацію захисту інформації, управління доступом, моніторинг безпеки та забезпечення надійної взаємодії між мережевими компонентами.

Мета роботи – аналіз та вивчення інструментів для захисту мережі, розроблення комп’ютерної системи, адміністрування захищеної корпоративної мережі з використанням сучасного мережевого обладнання та технологій безпеки, зокрема VLAN, ACL, криптографічного захисту, контролю доступу та моніторингу.

Проект складається з трьох розділів.

У першому розділі проаналізовано технічне завдання, структуру корпоративної мережі, сучасні мережеві технології та обладнання, необхідне для реалізації надійної та захищеної мережі.

Другий розділ присвячено аналізу засобів захисту: види систем захисту, контролю доступу, криптографії, антивірусного захисту та моніторингу, а також рекомендаціям щодо їх застосування в мережі.

У третьому розділі реалізовано модель захищеної мережі в Cisco Packet Tracer з використанням комутаторів Cisco CBS250/CBS350 та маршрутизатора Cisco RV340, з використанням VLAN, фільтрації трафіку та базового захисту.

У результаті роботи було розроблено концепцію захищеної корпоративної мережі, змодельовано її структуру, обґрунтовано вибір обладнання та засобів захисту, а також запропоновано рекомендації для подальшого адміністрування та масштабування системи.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧОК

DHCP – Протокол динамічної конфігурації хостів

DNS – Система доменних імен

IP – Інтернет-протокол

TCP/IP – Набір мережевих протоколів

MAC – Адреса управління доступом до середовища

VLAN – Віртуальна локальна мережа

ACL – Список контролю доступу

NAT – Перетворення мережевих адрес

VPN – Віртуальна приватна мережа

SSH – Захищена оболонка

RSA – Асиметричний алгоритм шифрування

SSL/TLS – Протоколи захищених з’єднань

IDS – Система виявлення вторгнень

IPS – Система запобігання вторгненням

SIEM – Управління інформацією та подіями безпеки

AAA – Аутентифікація, авторизація та облік

802.1X – Стандарт контролю доступу до портів у мережах

ISP – Інтернет-провайдер

GUI – Графічний інтерфейс користувача

CLI – Інтерфейс командного рядка

OS – Операційна система

LAN – Локальна мережа

WAN – Глобальна мережа

ВСТУП

У сучасному світі захист інформаційних та мережевих ресурсів є одним із головних завдань для корпоративних мереж. Зараз організації обробляють великі обсяги конфіденційної інформації, які потребують надійного захисту. Тому виникає необхідність ефективного адміністрування захищених корпоративних мереж, яке забезпечує надійне функціонування мережі, запобігає несанкціонованому доступу та мінімізує ризики втрати конфіденційної інформації.

Адміністрування захищеними системами включає впровадження безпеки на різних рівнях, управління користувачами та правами доступу, налаштування мережевого обладнання, системи виявлення загроз, засобів шифрування та оперативне втручання на негативні інциденти. Адміністрування має бути комплексним, що поєднує технологічні та організаційні аспекти захисту корпоративної мережі.

Метою проекту є вивчення принципів та методів ефективного адміністрування захищених систем у межах корпоративної мережі, аналіз сучасних засобів створення та захисту комп’ютерних систем, а також розгляд практичних рекомендацій ефективного адміністрування корпоративних мереж.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Корпоративна мережа

Корпоративна мережа – це комп’ютерна мережа, яка об’єднує різноманітні технічні пристрої в одну мережу для ефективної роботи підприємства, а також надійного захисту.

Комп’ютерна мережа — сукупність пристроїв, з’єднаних каналами передавання даних, для спільного користування апаратними, програмними та інформаційними ресурсами під керуванням спеціального програмного забезпечення.

Комп’ютерні мережі призначені для:

- швидкого обміну даними між окремими комп’ютерами даних;
- віддаленого керування комп’ютерами;
- спільного доступу до периферійних пристроїв.

У комп’ютерній мережі комп’ютери можуть виконувати різні функції. Комп’ютер, який керує розподілом ресурсів мережі, називають сервером, комп’ютери, які користуються ресурсами мережі, називають клієнтами, або робочими станціями[1].

Комп’ютерна мережа складається з інформаційних систем та каналів зв’язку. Під інформаційною системою розуміють об’єкт, здатний здійснювати

зберігання, обробку чи передачу інформації. До складу інформаційної системи входять: комп’ютери, програми, користувачі та інші складові, призначені для процесу обробки і передачі даних. Надалі інформаційна система, призначена для вирішення завдань користувача, називатиметься робоча станція. Під каналом зв’язку розуміють шлях чи засіб, по якому передаються сигнали. Засіб передачі сигналів називають абонентським, чи фізичним каналом.

Канали зв’язку створюються по лініях зв’язку за допомогою мережевого обладнання та фізичних засобів зв’язку. Фізичні засоби зв’язку

побудовані на основі кручених пар, коаксіальних кабелів, оптичних каналів або ефіру. Між взаємодіючими інформаційними системами через фізичні канали комунікаційної мережі та вузли комутації встановлюються логічні канали.

Логічний канал − це шлях для передачі даних від однієї системи до іншої. Логічний канал прокладається за маршрутом в одному або декількох фізичних каналах. Логічний канал можна охарактеризувати як маршрут, прокладений через фізичні канали і вузли комутації.

Інформація в мережі передається блоками даних за процедурами обміну між об’єктами. Ці процедури називають протоколами передачі даних.

Протокол − це сукупність правил, що встановлюють формат і процедури обміну інформацією між двома або кількома пристроями. Завантаження мережі характеризується параметром, що називається трафіком.

Трафік − це потік повідомлень в мережі передачі даних. Під ним розуміють кількісний вимір у вибраних точках мережі пройдених блоків даних і їх довжини, виражений в бітах за секунду.

Склад основних елементів у мережі залежить від її архітектури. Архітектура − це концепція, що визначає взаємозв’язок, структуру і функції взаємодії робочих станцій у мережі. Вона передбачає логічну, функціональну і фізичну організацію технічних та програмних засобів мережі. Архітектура визначає принципи побудови і функціонування апаратного та програмного забезпечення елементів мережі[2].

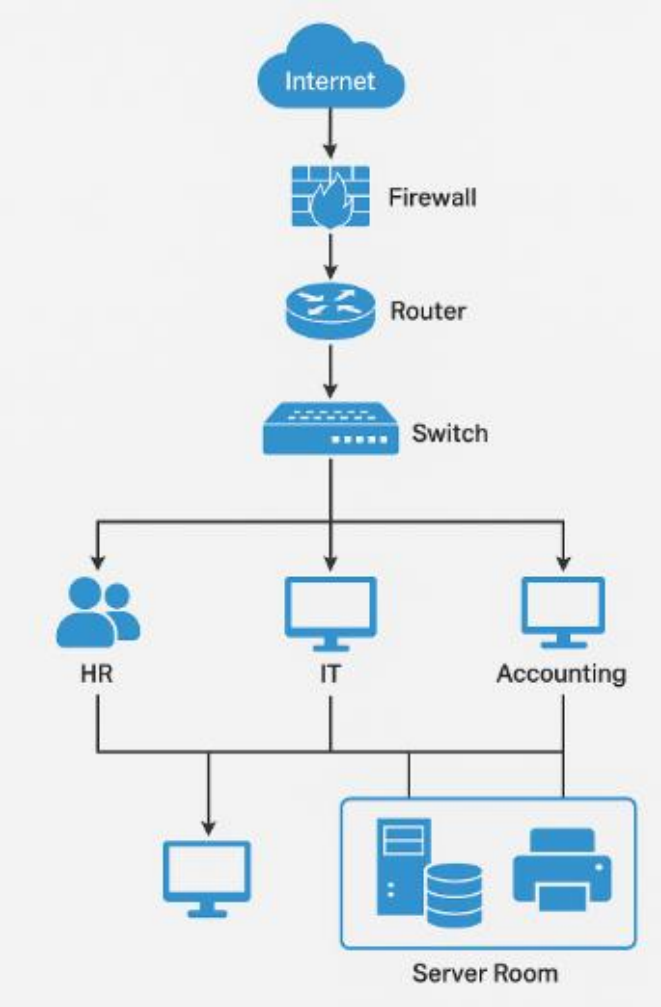

Рисунок 1.1 – Приклад корпоративної мережі

Корпоративні мережі являють собою взаємодію людей і комп'ютерів, який забезпечує ефективну передачу та обробку інформації. Робити мережу з комп'ютерами почали більше ніж 30 років тому та використовувались в різних сценаріях. Як тільки комп'ютери почали використовуватись масово та стали доступні кожному, розвиток мереж дуже прискорився.

1.2 Аналіз мережевих технологій

У сучасному світі мережеві технології відіграють важливу роль у забезпеченні ефективного функціювання підприємств та організацій.

Розвиток мережевих технологій сприяє не тільки підвищенню швидкості передачі даних, а й гарантуванню гнучкості, масштабованості та безпеки корпоративних мереж.

Комп'ютерні мережі класифікуються за топологією, за територією, за способом передачі інформації, за розподілом функцій.

Рисунок 1.2 – Класифікація комп'ютерних мереж

Персональні (PAN, від англ. Personal Area Network) — мережі для взаємодії пристроїв, що належать одній людині та об'єднують її власні електронні пристрої: персональні комп'ютери, ноутбуки, планшети, смартфони, комунікатори.

Локальні (LAN, від англ. Local Area Network) — з'єднують пристрої, розташовані на порівняно невеликій відстані один від одного, зазвичай у межах однієї або кількох сусідніх будівель, наприклад мережа навчального закладу.

Міські, регіональні (MAN, від англ. Metropolitan Area Network) — обласні й національні мережі.

Глобальні (WAN, від англ. Wide Area Network) — об'єднують комп'ютерні мережі. Найвідомішою глобальною мережею є Інтернет.

Топологією називають фізичне розташування вузлів мережі один відносно одного та способи їхнього з'єднання лініями зв'язку[1].

Існують три базові топології: загальна шина, кільце, зірка.

Топологія «загальна шина» передбачає використання одного кабелю, до якого під’єднуються всі комп’ютери мережі. Надіслане з будь-якого комп’ютера мережі повідомлення поширюється на всі інші комп’ютери мережі. Кожний із них перевіряє, кому адресовано повідомлення. Опрацьовує повідомлення лише той комп’ютер, якому воно адресоване. Комп’ютери можуть передавати дані лише послідовно, оскільки лінія зв’язку одна і спільна. Всі комп’ютери мають рівні права, все обладнання є ідентичним.

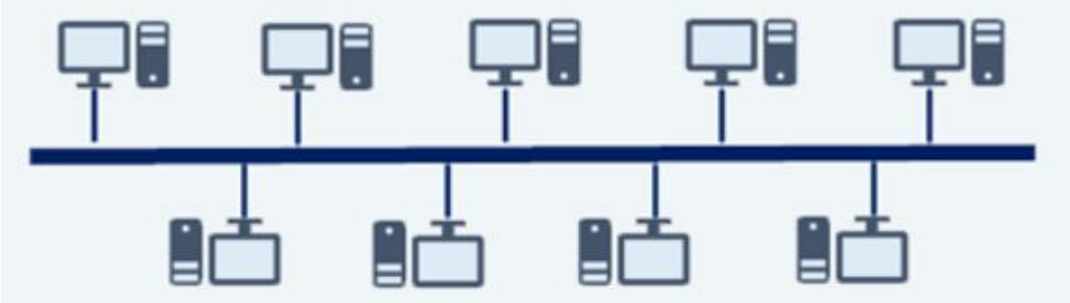

Рисунок 1.3 – Топологія «загальна шина»

Топологія «кільце» — топологія, в якій кожен комп’ютер з’єднано лініями зв’язку лише з двома іншими від одного він тільки отримує інформацію, а іншому тільки передає. Комп’ютери в «кільці» не є повністю рівноправними: одні обов’язково отримують інформацію від комп’ютера, який надсилає повідомлення в цей момент, раніше, а інші — пізніше.

Рисунок 1.4 – Топологія «кільце»

У топології «зірка» всі комп’ютери мережі приєднано до центрального

вузла, через який весь обмін інформацією йде від одного комп’ютера до іншого. Як центральний вузол можуть виступати або концентратор чи комутатор — таку топологію називають пасивною «зіркою», або потужний комп’ютер, на який покладається дуже велике навантаження, таку топологію називають активною «зіркою»[1].

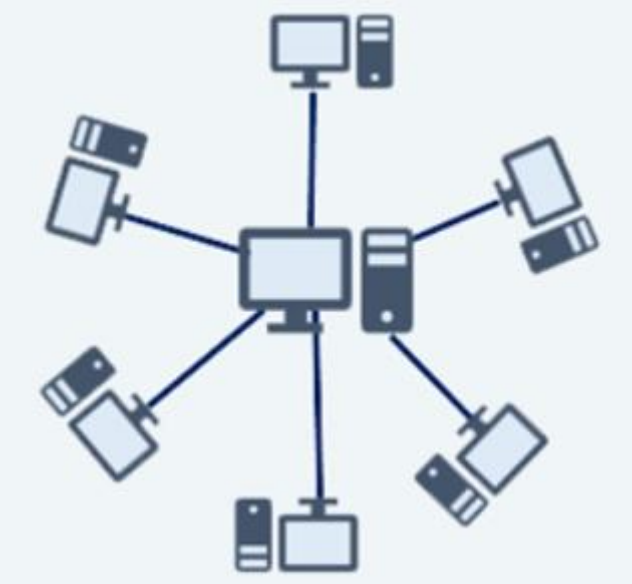

Рисунок 1.5 – Топологія «зірка»

За способом передавання даних мережі поділяють на кабельні і бездротові.

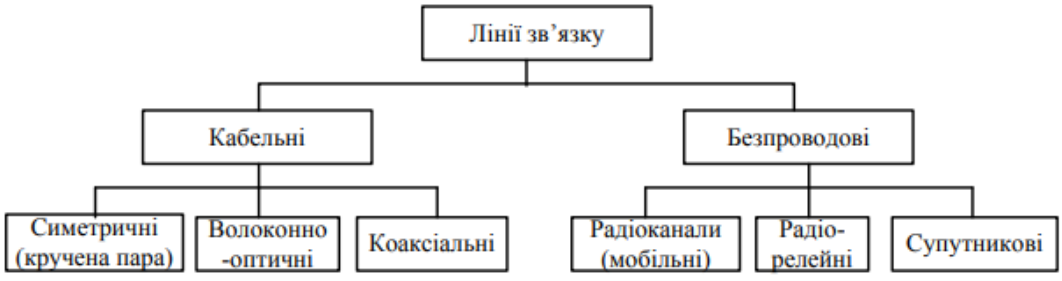

Рисунок 1.6 – Лінії зв’язку

Кабельною, називають мережу, у якої середовищем передавання даних є кабель. У такому середовищі дані передаються електричними або оптичними сигналами.

Є кілька видів кабелів, які використовують в комп'ютерній мережі – кручена пара, коаксіальний кабель, оптоволоконний кабель.

Кручена пара — це декілька пар скручених мідних дротів у кольоровій пластиковій ізоляції. Пучки кручених пар дротів захищає зовнішнє обплетення. Такий кабель використовують у телефонному зв'язку та в більшості мереж Ethernet — це пакетна технологія передачі даних, яка застосовується при побудові комп'ютерних мереж. Залежно від типу кабелю максимальна відстань передавання даних без підсилення сигналу становить від 15 до 100 м, а швидкість передавання даних може досягати 100 Гбіт/с.

Коаксіальний кабель — це кабель із ізольованою мідною оточеною металевою оболонкою-екраном. Такий кабель використовують для під'єднання комп'ютерів до мережі та поширення сигналів телебачення. Максималь- на відстань передавання даних без підсилення сигналу становить 500 м, максимальна швидкість передавання даних може досягати 10 Мбіт/с.

Оптоволоконний кабель — це скляна або пластикова нитка, що використовується для перенесення світла за допомогою повного внутрішнього відображення. Структура оптоволоконного кабелю схожа на структуру коаксіального кабелю. Але замість центрального мідного дроту в такому кабелі використовується тонке (діаметром близько 1–10 мкм) оптоволокно, а замість внутрішньої ізоляції — скляна або пластикова оболонка, що не дозволяє світлу виходити за межі оптоволокна[1].

Оптоволоконний кабель є найкращим вирішенням для застосування. Він найшвидший на сьогодні спосіб передавання даних. Має велику відстань передавання даних до 50 км, а швидкість передавання даних сягає від 10 Гбіт/с до 4–8 Тбіт/с.

Бездротова мережа – це мережа, в якій дані передаються радіосигналами. Є декілька стандартних бездротових мереж.

Wi-Fi (від англ. Wireless Fidelity) — стандарт для обладнання бездротових мереж і торгова марка консорціуму Wi-Fi Alliance, до якого входять найбільші виробники комп'ютерного устаткування та обладнання Wi-Fi.

WiMAX, Mobile WiMAX, Mobile-Fi — технології бездротових мереж, які призначено для використання разом із технологією Wi-Fi (або замість неї) із метою розширення бездротових мереж. Зокрема, мережа WiMAX забезпечує кращий доступ до Інтернету, ніж Wi-Fi, і має більшу площу покриття. LTE (від англ. Long-Term Evolution) — стандарт бездротової високо швидкісної передачі даних для мобільних телефонів і інших терміналів, що працюють із даними.

Bluetooth — стандарт для бездротових персональних мереж. Технологія забезпечує обмін даними між кишеньковими та стаціонарними комп'ютерами, мобільними телефонами, ноутбуками, принтерами, цифровими фотокамерами тощо[1].

Загальна характеристика стека протоколів TCP/IP. Протокол IP був розроблений у 1970-их роках минулого сторіччя при проектуванні мережі ARPANET міністерства оборони США та вдосконалений у вісімдесяті роки на початку розвитку всесвітньої комп'ютерної мережі Internet. Internet із самого початку проектувався як інтегрована високонадійна територіально розподілена мережа, яка об'єднує велику кількість комп'ютерів з різним апаратним забезпеченням. І саме такою мережею він залишається зараз. Така мережа повинна мати апаратно незалежний стек протоколів. Тут першою серйозною проблемою є ідентифікація вузлів мережі, яка проводиться через числову систему адрес. Чотирирівнева ієрархічна адресація з можливістю зміни числових адрес на кожному з цих рівнів від 0 до 255 дає змогу організувати надання адрес комп'ютерам таким чином, що кожен з них навіть у масштабах світу буде мати унікальну ієрархічну адресу. Вдало

підібраний механізм адресації, а також апаратна та системна прозорість сприяли тому, що сьогодні TCP/IP став універсальним міжмережевим протоколом. Тому систему числових адрес комп'ютерів назвали IP-адресами.

Реєстрація IP адрес та пошук маршрутів у мережі забезпечують сервіси мережевого та транспортного рівнів TCP/IP. Зрозуміло, що в інших протоколах мережевого та транспортного рівня використовується своя система адрес. Але ці протоколи не знайшли такого широкого поширення і не забезпечують необхідної апаратної та системної прозорості. Так, протокол NetBios використовується тільки під ОС Microsoft Windows, тоді як протокол IPX − тільки серверною операційною системою Novell NetWare. Крім того, стандарти цих протоколів належать фірмам-виробникам. А протокол TCP/IP створювався іншим чином. Перші його реалізації розроблялися під ОС UNIX [8], яка була і залишається апаратно незалежною системою. ОС UNIX, яку розробляла та вдосконалювала у демократичній манері група ентузіастів американських університетів, не стала комерційною системою і сьогодні. Демократизм і відкритість UNIX перейняв і протокол TCP/IP, увібравши всі його стандарти та документацію.

Але найважливішим чинником розвитку TCP/IP як єдиного всесвітнього стандарту міжмережевого протоколу стала масштабованість та апаратна незалежність системи адрес мережевого рівня[2].

1.3 Аналіз мережевого обладнаня

Для побудови ефективної та захищеної корпоративної мережі одним із ключових етапів є аналіз та вибір відповідного мережевого обладнання. Обрана апаратна база повинна забезпечувати як продуктивність, так і можливості з реалізації засобів безпеки, таких як сегментація, контроль доступу, VPN-захист, моніторинг тощо. Основні види мережевого

обладнання включають комутатори, маршрутизатори, точки доступу, міжмережеві екрани, мережеві адаптери, модеми та контролери бездротової мережі.

Мережеві адаптери − це мережеве устаткування, що забезпечує функціонування мережі на фізичному і канальному рівнях.

Рисунок 1.7 – Мережевий адаптер

Мережевий адаптер відноситься до периферійного пристрою комп'ютера, безпосередньо взаємодіє із середовищем передачі даних, яке прямо чи через інше комунікаційне обладнання пов'язує його з іншими комп'ютерами. Цей пристрій розв'язує завдання надійного обміну двійковими даними, поданими відповідними електромагнітними сигналами, по зовнішніх лініях зв'язку. Як і будь-який контролер комп'ютера, мережевий адаптер працює під управлінням драйвера операційної системи, і розподіл функцій між мережевим адаптером та драйвером може змінюватися від реалізації до реалізації. Комп'ютер, чи то сервер, чи робоча станція, підключається до мережі за допомогою внутрішньої плати − мережевого адаптера (хоча бувають й зовнішні мережеві адаптери, що підключаються до комп'ютера через паралельний порт). Мережевий адаптер вставляється в гніздо материнської плати. Карти мережевих адаптерів встановлюються на кожній робочій станції та на файловому сервері. Робоча станція відправляє

запит до файлового сервера і отримує відповідь через мережевий адаптер, коли файловий сервер готовий. Мережеві адаптери перетворюють паралельні коди, що використовуються всередині комп'ютера та подані малопотужними сигналами, в послідовний потік потужних сигналів для передачі даних по зовнішній мережі. Мережеві адаптери повинні бути сумісні з кабельною системою мережі, внутрішньою інформаційною шиною ПК і мережевою операційною системою.

Перші пристрої, що дозволяли об'єднувати кілька мереж, були двопортовими і отримали назву мостів. З розвитком даного типу обладнання вони стали багатопортовими і отримали назву комутаторів. Певний час обидва поняття існували одночасно, а пізніше замість терміна «міст» стали застосовувати «комутатор». Міст, а також його швидший аналог – комутатор, поділяють загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання кількох фізичних сегментів (відрізків кабелю) за допомогою одного чи кількох концентраторів.

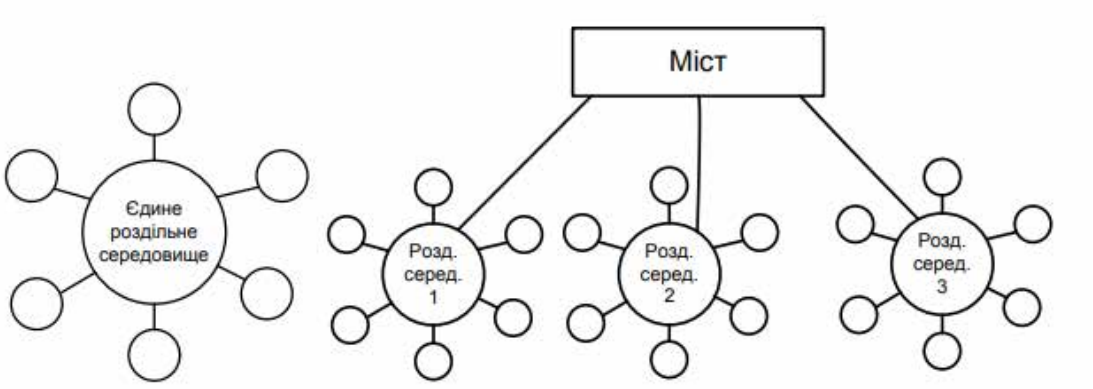

Рисунок 1.8 – Схема мосту

Кожен логічний сегмент підключається до окремого порту моста. Після надходження кадру на певний порт міст повторює цей кадр, але не на всіх портах, як це робить концентратор, а тільки на тому порті, до якого під'єднано сегмент, що містить комп'ютер-адресат. Тим самим міст ізолює трафік одного сегмента від трафіку іншого, і підвищує загальну

продуктивність мережі. Локалізація трафіку не лише економить пропускну здатність, але і знижує можливість несанкціонованого доступу до даних, оскільки кадри не виходять за межі свого сегмента і їх складніше перехопити зловмисникові.

Комутатор за функціональністю є подібним до моста і відрізняється від моста, в основному, вищою продуктивністю. Кожен порт комутатора оснащено спеціальним процесором, який обробляє кадри за алгоритмом моста незалежно від процесорів інших портів. Міст в кожен момент часу може здійснювати передачу кадрів тільки між однією парою портів, а комутатор одночасно підтримує потоки даних між всіма своїми портами. Іншими словами, міст передає кадри послідовно, а комутатор паралельно.

Мости з'явилися в ті часи, коли мережу ділили на невелику кількість сегментів, а міжсегментний трафік був невеликим. Мережу найчастіше ділили на два сегменти, тому і термін був вибраний відповідний − міст. Для обробки потоку даних з середньою інтенсивністю 1 Мбіт/с мосту цілком вистачало продуктивності одного процесорного блока. При зміні ситуації в кінці 80-х – початку 90-х років − появі швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації, розділенні мережі на велику кількість сегментів − класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між кількома портами за допомогою одного процесорного блока потребувало значного підвищення швидкодії процесора і було досить дорогим рішенням.

Ефективнішим виявилося рішення, яке і «породило» комутатори: для обслуговування потоку, що надходить на кожен порт, в пристрій ставився окремий спеціалізований процесор, який реалізовував алгоритм моста. За своєю суттю, комутатор − це мультипроцесорний міст, здатний паралельно просувати кадри відразу між всіма парами своїх портів.

Коли стало економічно виправдано використовувати окремі спеціалізовані процесори на кожному порту комунікаційного пристрою, комутатори локальних мереж повністю витіснили мости. За рахунок цього

загальна продуктивність комутатора зазвичай є вищою за продуктивність традиційного моста, що має один процесорний блок.

В комунікаційній мережі комутатор є системою ретрансляції − системою, що призначена для передачі даних або перетворення протоколів. Комутація здійснюється тут без жодної обробки даних.

Комутатор не має буферів і не може накопичувати дані. Тому при використанні комутатора швидкості передачі сигналів в каналах мають збігатися. Канальні процеси, що реалізовуються комутатором, виконують спеціальні інтегральні схеми.

Спочатку комутатори використовувалися лише в територіальних мережах. Потім вони з'явилися і в локальних мережах, наприклад, комутатори приватних установ. Пізніше з'явилися комутовані локальні мережі, їх ядром стали комутатори локальних мереж. Комутатор може об'єднувати сервери і бути основою для об'єднання кількох робочих груп. Він скеровує пакети даних між вузлами локальної мережі. Кожен комп'ютер сегмента отримує доступ до каналу передачі даних без конкуренції і бачить лише той трафік, який курсує в його сегменті.

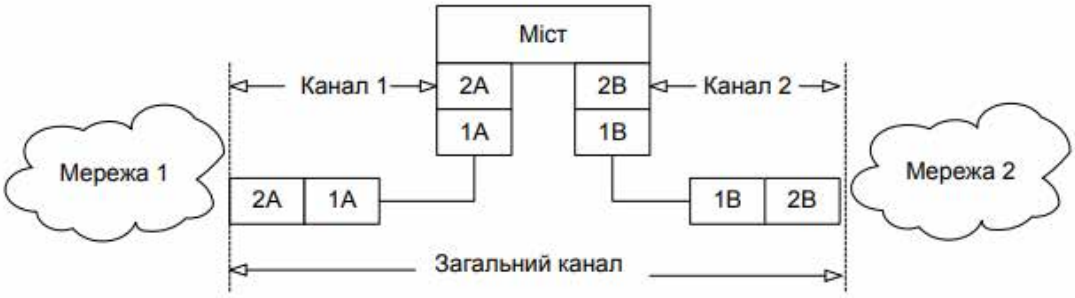

Рисунок 1.9 – Поєднання двох мереж за допомогою двох каналів

Маршрутизатор – система ретрансляції, що сполучає дві комунікаційні мережі або їх частини. Маршрутизатори працюють на третьому (мережевому) рівні моделі OSI, що взаємодіє з протоколами вищих рівнів.

Маршрутизатори, як і мости або комутатори, ретранслюють пакети з однієї частини мережі в іншу. Спочатку маршрутизатор від моста відрізнявся тільки тим, що на комп'ютері, який об'єднує дві чи більшу кількість мереж, було встановлено інше програмне забезпечення. Сьогодні між маршрутизатором і мостом існують принципові відмінності, маршрутизатори працюють не з фізичними адресами пакетів (MACадресами), а з логічними мережевими адресами (IP-адресами). Маршрутизатори ретранслюють не всю інформацію, що приходить, а тільки ту, яка адресована до них особисто, і відкидають (не ретранслюють) широкомовні пакети, маршрутизатори, на відміну від мостів і комутаторів, не є прозорими для абонентів. Головною відмінністю є те, що маршрутизатори підтримують мережі з великою кількістю можливих маршрутів та шляхів передачі інформації, так звані комірчасті мережі (meshed networks). Мости ж потребують, щоб в мережі не було петель, щоб шлях поширення інформації між двома будь-якими абонентами був єдиним.

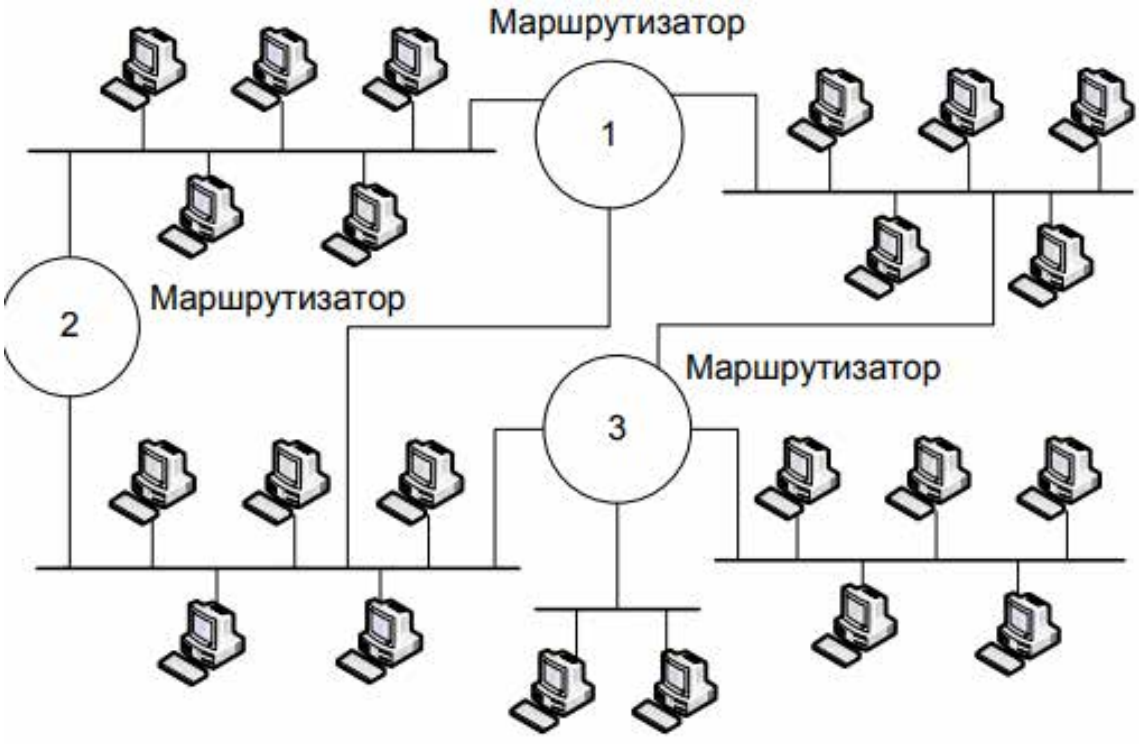

Рисунок 1.10 – Комірчаста мережа з маршрутизаторами

Маршрутизатори є складнішими за мости і комутатори і, відповідно, дорожчими. Маршрутизаторами складніше управляти, вони є повільнішими за комутатори. Проте, вони забезпечують найглибше розділення мережі на частини.

Якщо концентратори лише повторюють всі пакети (фізичний рівень моделі OSI), що надійшли на них, комутатори і мости ретранслюють тільки міжсегментні і широкомовні пакети (канальний рівень), то маршрутизатори сполучають окремі автономні мережі, що не впливають одна на одну, зберігаючи при цьому можливість передачі інформації між ними (мережевий рівень).

Розмір мережі, що під'єднується до маршрутизатора, практично нічим не обмежено: ні допустимими розмірами зони конфліктів, ні допустимою кількістю широкомовних пакетів, ні можливими для комутаторів і мостів різноманітними перевантаженнями. При цьому легко забезпечуються альтернативні, дублюючі шляхи поширення інформації для збільшення надійності зв'язку.

Маршрутизатори обробляють адресну інформацію, що міститься у службовій інформації пакета. Вона містить номер мережі, і саме ці мережі сполучає маршрутизатор.

Кожен абонент, перш ніж відправити пакет, визначає, чи може він скерувати його безпосередньо до одержувача, чи йому потрібно скористатися послугами маршрутизатора. Якщо номер власної мережі відправника збігається з номером мережі отримувача, то пакет передається безпосередньо, без маршрутизації. Якщо отримувач знаходиться в іншій мережі, то пакет передається до маршрутизатора, який скеровує його у потрібну мережу. При цьому виходить, що пакет в цілому адресовано до маршрутизатора (як до одного з абонентів власної мережі), а вкладена в ньому інформація адресована абоненту з іншої мережі, для якого вона, власне, і призначена.

Маршрутизатор аналізує IP-адресу, що міститься у складі пакета, і перетворює пакет, що надійшов по одній з мереж, на пакет, що призначений для іншої мережі. У полі адреси пакета він ставить MAC-адресу одержувача і свою MAC-адресу, як відправника пакета. У відповідь пакет аналогічно має пройти через посередника – маршрутизатор.

Саме маршрутизатори найчастіше використовуються для зв'язку локальних мереж з глобальними, зокрема, з Інтернет, яка може розглядатися як мережа, що повністю маршрутизована.

Шлюз (gateway) – ретрансляційна система, що забезпечує взаємодію інформаційних мереж. Шлюз дозволяє об'єднувати мережі, що побудовані на істотно різних програмних і апаратних платформах. Наприклад, шлюз може дозволити користувачам, що працюють в мережі Unix, взаємодіяти з користувачами мережі Windows. Шлюзи оперують на верхніх рівнях моделі OSI (сеансовому, представницькому і прикладному) і є найбільш розвиненим методом під'єднання мережевих сегментів і комп'ютерних мереж. Необхідність в мережевих шлюзах виникає при об'єднанні двох систем, що мають різну архітектуру. Як шлюз зазвичай використовується виділений комп'ютер, на якому запущено програмне забезпечення шлюзу і здійснюються перетворення, що дозволяють взаємодіяти кільком системам у мережі. Іншою функцією шлюзів є перетворення протоколів. При отриманні повідомлення IPX/SPX для клієнта TCP/IP шлюз перетворює повідомлення на протокол TCP/IP. Шлюзи складні в установленні та налаштуванні. Шлюзи працюють повільніше, ніж маршрутизатори[2].

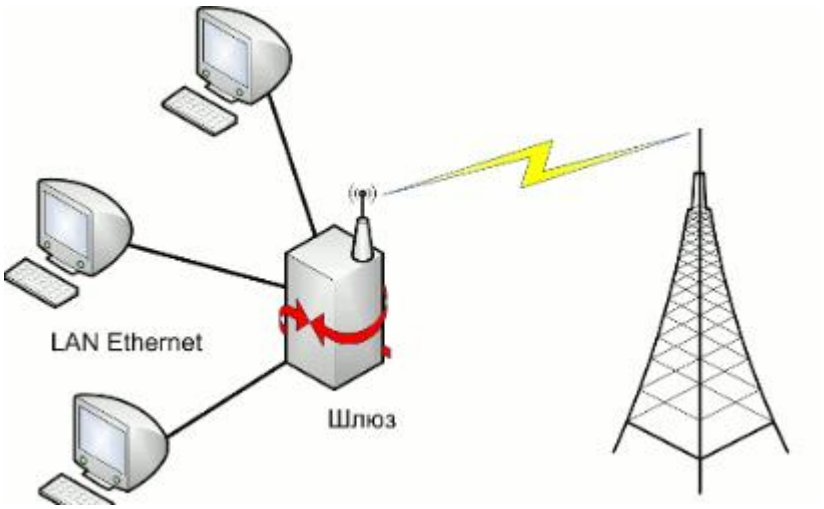

Рисунок 1.11 – Робота шлюзу

1.4 Аналіз завдання проекту

У сучасних корпоративних мережах інформаційна безпека є одним з головних пріоритетів. З кожним роком збільшуються кіберзагрози, тому адміністрування мережі без належного захисту є вкрай ризикованим. Проект зосереджений на аналізі та реалізації захисту систем, що функціонують в межах корпоративної інфраструктури.

Завданням цього проекту є розробка та впровадження безпечного простору для адміністрування комп'ютерних систем в рамках корпоративної мережі. Це передбачає конфігурування мережевої інфраструктури з урахуванням політик безпеки, забезпечення криптографічного захисту передачі даних, обмеження доступу до адміністративних ресурсів та впровадження методів контролю й моніторингу доступу. Обрати програмні та апаратні методи безпеки для реалізації захищеної мережі. Проаналізувати політику безпеки для корпоративної мережі. Надати рекомендації щодо адміністрування та супроводу захищеної системи.

Провести моделювання системи в програмному середовищі Cisco Packet Tracer та налаштувати безпеку мережі.

2 АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ МЕРЕЖІ

2.1 Види систем захисту

Захист мережі — це комплекс заходів і засобів, що забезпечують конфіденційність, цілісність та доступність даних, а також запобігають несанкціонованому доступу. Основні категорії систем захисту включають: системи контролю доступу, криптографічний захист, мережева безпека, антивірусні платформи та захист кінцевих пристроїв та моніторинг безпеки.

Системи контролю доступу – відповідають за ідентифікацію користувачів і визначення їх прав у мережі. Вони регулюють, хто може входити в систему, які ресурси доступні кожному користувачу та які дії дозволені. Основу складають механізми автентифікації (логін/пароль, токени, біометрія) та авторизації (розподіл прав доступу).

Криптографічний захист – забезпечує конфіденційність і цілісність даних за допомогою шифрування. Він дозволяє передавати інформацію навіть через відкриті мережі, не боячись її перехоплення. Сучасні алгоритми, такі як AES, RSA чи ECC, широко використовуються в VPN-з'єднаннях, електронному підписі, протоколах IPsec та SSL/TLS. Завдяки криптографії навіть у разі перехоплення даних вони залишаються непридатними без відповідного ключа дешифрування.

Мережева безпека – включає сукупність технічних засобів і правил, що захищають інфраструктуру від атак та несанкціонованого доступу. Серед ключових елементів — міжмережеві екрани (firewalls), системи виявлення вторгнень (IDS) і системи запобігання (IPS), які аналізують трафік і блокують загрози в реальному часі. Додатково використовується сегментація мережі (VLAN), що ізолює чутливі частини інфраструктури, зменшуючи зону ураження при атаці.

Антивірусни платформи та захист кінцевих пристроїв системи захищають персональні комп'ютери, ноутбуки, мобільні пристрої та інші кінцеві точки від шкідливого ПЗ. Вони включають антивірусні програми, фаерволи, фільтри шкідливих веб-сайтів, а також рішення для моніторингу активності (EDR). Завдяки ним вдається виявляти шпигунське ПЗ та інші загрози, ще до того, як вони завдадуть шкоди системі. Це критично важливо, адже саме через кінцеві пристрої найчастіше здійснюються кібератаки.

Моніторинг безпека – забезпечують постійне спостереження за станом мережі, подіями та потенційними загрозами. Вони дозволяють оперативно реагувати на підозрілу активність, відстежувати вторгнення, проводити аналіз інцидентів. Найчастіше використовуються SIEM-системи, які централізовано збирають і аналізують логи з усіх компонентів мережі. Аудит безпеки, у свою чергу, дозволяє регулярно перевіряти відповідність налаштувань стандартам та політикам організації.

2.2 Системи контролю доступу

Контроль доступу – це процес захисту даних, який дозволяє організаціям керувати тим, хто має право доступу до корпоративних даних і ресурсів. Безпечний контроль доступу використовує функції, які

перевіряють, чи є користувачі тими, за кого вони себе видають, і гарантує, що користувачам надаються відповідні рівні доступу.

Існує чотири основні типи контролю доступу, кожен з яких керує доступом до конфіденційної інформації унікальним чином.

1. Контроль доступу на основі атрибутів (ABAC)

ABAC — це динамічна, контекстно-орієнтована політика, яка визначає доступ на основі прав доступу, наданих користувачам. Система використовується в системах керування ідентифікацією та доступом (IAM).

2. Дискреційний контроль доступу (DAC)

Моделі DAC дозволяють власнику даних вирішувати питання контролю доступу, призначаючи права доступу правилам, які визначають користувачі. Коли користувачеві надається доступ до системи, він може надавати доступ іншим користувачам, як вважає за потрібне.

3. Обов'язковий контроль доступу (MAC)

MAC встановлює суворі правила для окремих користувачів та даних, ресурсів і систем, до яких вони хочуть отримати доступ. Ці правила керуються адміністратором організації. Користувачі не можуть змінювати, скасовувати або встановлювати дозволи.

4. Контроль доступу на основі ролей (RBAC)

RBAC створює дозволи на основі груп користувачів, ролей, які виконують користувачі, та дій, які вони виконують. Користувачі можуть виконувати будь-які дії, дозволені для їхньої ролі, і не можуть змінювати призначений їм рівень контролю доступу[3].

2.3 Криптографічний захист

Єдиний логічний спосіб захистити інформацію –зашифрувати її. Криптографія – це практика дослідження захисту комунікації таким чином,

щоб тільки той, кому призначене повідомлення, міг його зрозуміти. Шифрування мережевого трафіку настільки поширене, що більшість людей навіть не підозрюють, що воно регулярно використовується для шифрування зв'язку між веб-серверами і клієнтами, які до них підключаються, у вигляді протоколів Secure Sockets Layer (SSL) і Transport Layer Security (TLS).

Мережева безпека зазвичай стосується всіх заходів, вжитих для захисту комп'ютерної мережі та інформації організації. Завдання полягає в тому, щоб забезпечити доступ до даних у мережі для всіх, хто їх потребує, одночасно захищаючи їх від сторонніх очей.

Існує велика кількість протоколів, пристроїв і технологій, призначених для захисту комп'ютерних мереж. Сучасна мережева архітектура є складною та стикається з постійно новим середовищем загроз і зловмисниками, які постійно шукають і намагаються використати недоліки в різних місцях, включаючи обладнання, дані, програми та людей. Як результат, сьогодні використовуються численні системи та програми управління мережевою безпекою , які вирішують регуляторні питання, а також конкретні загрози та експлойти.

Криптографія запобігає несанкціонованому доступу до конфіденційної інформації, що зберігається або передається, роблячи її незрозумілою без правильного ключа. Вона використовує шифрування для захисту передачі даних через мережі, гарантуючи, що лише ті, хто має авторизовані ключі, можуть отримати доступ до зашифрованих даних. Будь-яка криптографічна система включає як алгоритм (у криптографії багато математики), так і ключ. Хитрощі в тому, що система має бути безпечною, навіть якщо все, крім ключа, є загальновідомим. Ви можете визначити вимоги вашої організації до криптографії залежно від структури, вже впроваджених заходів безпеки та загального управління.

Хоча використовується багато різних типів криптографічних алгоритмів, їх можна розділити на три групи: симетрична криптографія, асиметрична криптографія, хеш-функції.

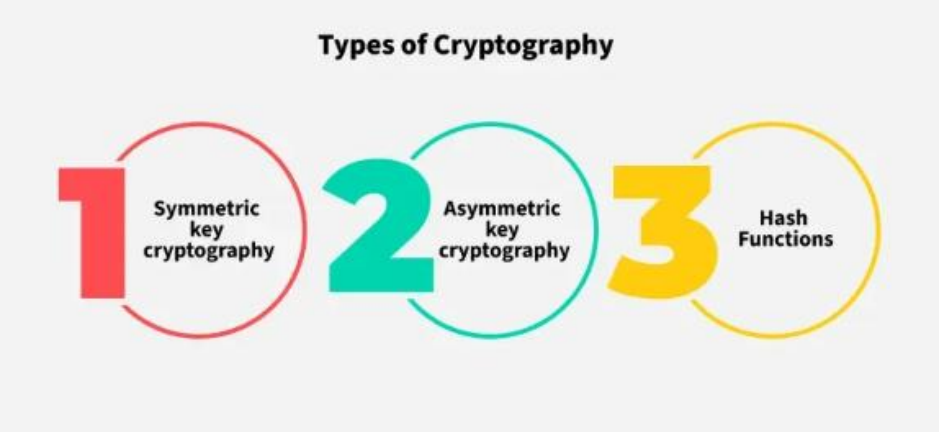

Рисунок 2.1 – Типи криптографії

Симетрична криптографія – відправник, так і одержувач використовують один і той самий ключ для шифрування та розшифрування повідомлень. Одним із поширених застосувань симетричної криптографії є захист жорсткого диска – зазвичай це один і той самий користувач, який записує та читає дані з жорсткого диска, тому немає проблем із обміном ключем з ким завгодно.

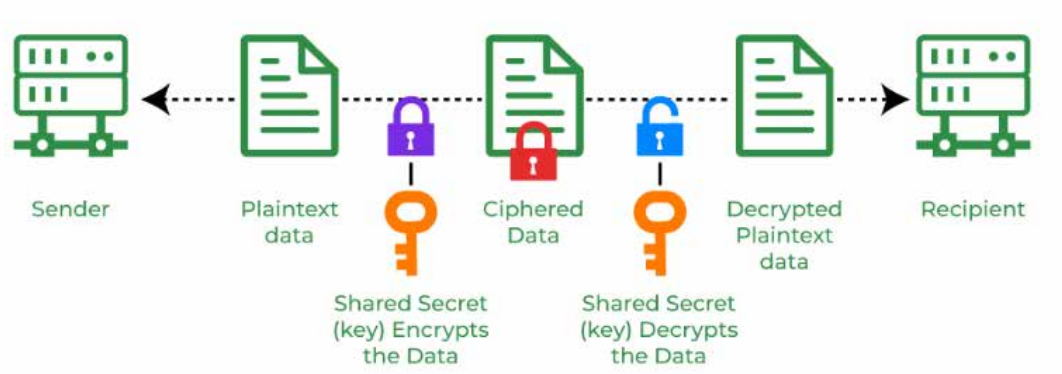

Рисунок 2.2 – Робота симетричної криптографії

Асиметрична криптографія, яку також називають криптографією з відкритим ключем, полягає в тому, що кожна особа, яка бере участь у перетворенні, має два ключі: один відкритий і один закритий. Відкритий ключ може бути оприлюднений усім світом, тоді як закритий ключ має залишатися в таємниці. Ці два ключі пов'язані таким чином, що повідомлення, зашифровані відкритим ключем, можна розшифрувати за

допомогою закритого ключа. За допомогою цієї системи лише цільовий одержувач повідомлення (той, хто має правильний закритий ключ) може розшифрувати повідомлення, зашифровані за допомогою його відкритого ключа. Система працює, доки відкритий ключ підключено до правильної особи. Щоб забезпечити роботу з'єднання, можна використовувати сторонні системи, такі як інфраструктура відкритих ключів та довірені джерела, відомі як центр сертифікації.

Рисунок 2.3 – Робота асиметричної криптографії

Хеш-фукнції використовують, щоб перетворити повідомлення будь-якої довжини або типу на зашифрований текст фіксованої довжини. Процес є одностороннім – немає способу скасувати шифрування та повернути оригінальне повідомлення.

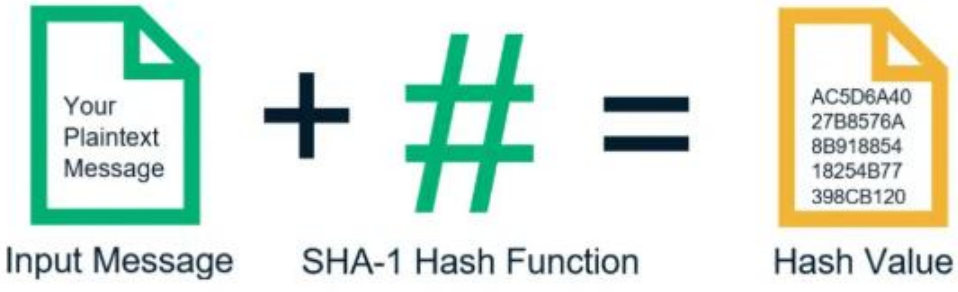

Рисунок 2.4 – Робота хеш-фукнції

Хеш-функції корисні, оскільки результуючий хеш унікальний для кожного блоку зашифрованої інформації. Це означає, що хеш можна

використовувати для перевірки цілісності вихідного блоку інформації – якщо щось у цій інформації змінилося, пропуск її через ту саму хеш-функцію призведе до іншого хешу[11].

Рисунок 2.5 – Алгоритм роботи хешу

Криптографія має широку сферу застосування в сучасному світі, де технології швидко розвиваються. Від засобів автентифікації до криптовалют, криптографія залишається з нами. Нижче наведено деякі з найпоширеніших застосувань криптографії:

Комп'ютерні паролі: криптографія широко використовується в комп'ютерній безпеці, особливо під час створення та підтримки паролів. Коли користувач входить у систему, його пароль хешується та порівнюється з хешем, який зберігався раніше. Паролі хешуються та шифруються перед збереженням. За допомогою цієї техніки паролі шифруються таким чином, що навіть якщо хакер отримає доступ до бази даних паролів, він не зможе їх прочитати.

Цифрові валюти: для захисту транзакцій та запобігання шахрайству цифрові валюти, такі як Bitcoin, також використовують криптографію. Для захисту транзакцій використовуються складні алгоритми та криптографічні ключі, що робить їх підробку або маніпуляції майже неможливими.

Безпечний перегляд веб-сторінок: безпека перегляду веб-сторінок забезпечується використанням криптографії, яка захищає користувачів від підслуховування та атак типу «людина посередині». Криптографія з відкритим
ключем використовується протоколами Secure Sockets Layer (SSL) та Transport Layer Security (TLS) для шифрування даних, що надсилаються між веб-сервером і клієнтом, створюючи безпечний канал зв'язку.

Електронні підписи: електронні підписи слугують цифровим еквівалентом власноручного підпису та використовуються для підписання документів. Цифрові підписи створюються за допомогою криптографії та можуть бути перевірені за допомогою криптографії з відкритим ключем. У багатьох країнах електронні підписи є обов'язковими до виконання законом, і їх використання швидко розширюється.

Автентифікація: криптографія використовується для автентифікації в багатьох різних ситуаціях, таких як доступ до банківського рахунку, вхід у комп'ютер або використання захищеної мережі. Криптографічні методи використовуються протоколами автентифікації для підтвердження особи користувача та підтвердження того, що він має необхідні права доступу до ресурсу.

Криптовалюти: криптографія активно використовується криптовалютами, такими як Bitcoin та Ethereum, для захисту транзакцій, запобігання шахрайству та підтримки цілісності мережі. Для захисту транзакцій використовуються складні алгоритми та криптографічні ключі, що робить їх підробку або маніпуляції практично неможливими.

Наскрізне інтернет-шифрування: наскрізне шифрування використовується для захисту двостороннього зв'язку, такого як відеодзвінки, миттєві повідомлення та електронна пошта. Навіть якщо повідомлення зашифроване, це гарантує, що його зможуть прочитати лише цільові одержувачі. Наскрізне шифрування широко використовується в таких

комунікаційних програмах, як WhatsApp і Signal, і забезпечує високий рівень безпеки та конфіденційності для користувачів.

Алгоритми криптографії можна класифікувати на кілька категорій залежно від способу використання та управління ключами, їхньої ефективності та робочого процесу. Ось найпоширеніші алгоритми.

Розширений стандарт шифрування (AES) – це популярний алгоритм шифрування, який використовує один і той самий ключ для шифрування та дешифрування. Це симетричний алгоритм блокового шифрування з розміром блоку 128 біт, 192 біти або 256 біт. Алгоритм AES широко вважається заміною алгоритму DES (Data encryption standard).

Стандарт шифрування даних (DES) – це старіший алгоритм шифрування, який використовується для перетворення 64-бітних даних відкритого тексту на 48-бітний зашифрований шифротекст. Він використовує симетричні ключі (що означає один і той самий ключ для шифрування та дешифрування). Він дещо старий за сучасними стандартами, але може бути використаний як базовий структурний блок для вивчення новіших алгоритмів шифрування.

RSA — це базовий асиметричний криптографічний алгоритм, який використовує два різні ключі для шифрування. Алгоритм RSA працює за концепцією блочного шифру, який перетворює звичайний текст у зашифрований текст і навпаки.

Алгоритм безпечного хешування (SHA) використовується для створення унікальних цифрових відбитків вхідних даних фіксованої довжини, відомих як хеші . Варіації SHA, такі як SHA-2 та SHA-3, зазвичай використовуються для забезпечення цілісності та автентичності даних. Найменша зміна вхідних даних суттєво змінює результат хешування, що вказує на втрату цілісності. Хешування – це процес зберігання пар ключ-значення за допомогою хеш-функції в хеш-таблицю.

Криптографія використовується для захисту інформації та комунікацій шляхом перетворення даних у закодовані формати, забезпечення

конфіденційності, цілісності та автентифікації. Вона є важливою для широкого кола застосувань, включаючи захист онлайн-транзакцій, перегляд веб-сторінок, паролів, цифрових валют та автентифікацію.

Криптографія постійно розвивається, щоб випереджати загрози безпеці, пропонуючи такі рішення, як шифрування із симетричним ключем (AES), шифрування із асиметричним ключем (RSA) та хеш-функції (SHA) для забезпечення конфіденційності та цілісності даних.

Завдяки широкому застосуванню в таких галузях, як безпечний перегляд веб-сторінок, криптовалюти, електронні підписи та наскрізне шифрування, криптографія відіграє життєво важливу роль у захисті конфіденційних даних від зловмисників. Оскільки цифрові загрози продовжують зростати, криптографія гарантує, що лише уповноважені сторони можуть отримувати доступ до критично важливої інформації, змінювати її або безпечно передавати[12].

2.4 Мережева безпека

Мережевий захист має різні компоненти захисту, такі як Firewalls, IDS/IPS та VPN.

Брандмауер(Firewalls) – це пристрій мережевої безпеки, розміщений на периметрі корпоративної мережі. Це робиться для того, щоб усі пакети, що надходять у мережу, спочатку проходили через брандмауер.

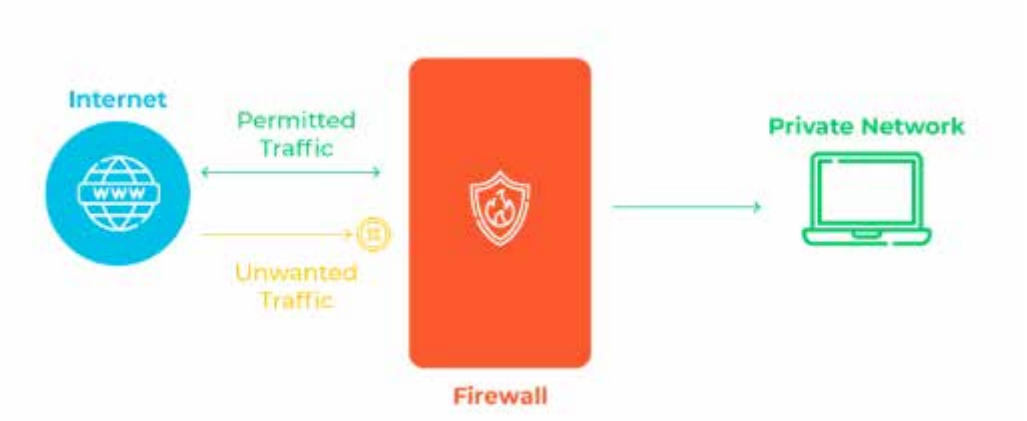

Рисунок 2.6 – Робота брандмауеру

Основна функція брандмауера полягає у фільтрації всіх пакетів, що входять, виходять та проходять через мережу, щоб запобігти несанкціонованому доступу між двома або більше комп'ютерами. Брандмауер сканує всі пакети та відповідно дозволяє, забороняє або відкидає їх, залежно від налаштованих на ньому правил. Наприклад, брандмауер може мати правила, налаштовані на дозвіл лише HTTP-пакетів. Якщо брандмауер отримує ICMP-пакет, він просто відкидає його та не дозволяє йому ввійти в мережу.

Зазвичай використовуються два типи брандмауерів.

Мережевий брандмауер: ці брандмауери функціонують на мережевому рівні. Вони обробляють усі пакети, що входять та виходять з мережі, і фільтрують трафік на основі правил, налаштованих на брандмауері.

Брандмауер на базі хоста: Брандмауери на базі хоста встановлюються на персональному комп’ютері/ПК. Таким чином, цей брандмауер фільтрує весь трафік для однієї виділеної системи, на відміну від мережевих, які обслуговують усю мережу. Це програмні брандмауери, які зазвичай входять до складу операційної системи[4].

Система виявлення вторгнень (IDS) виявляє потенційні загрози та слабкі місця в мережевих системах. IDS аналізує мережевий трафік, попереджаючи адміністраторів про підозрілу активність, не втручаючись у передачу даних.

Рисунок 2.7 – Робота системи виявлення вторгнень

Системи виявлення вторгнень (IDS) розташовані поза основним потоком трафіку. Зазвичай вони працюють шляхом відзеркалювання трафіку для оцінки загроз, зберігаючи продуктивність мережі шляхом аналізу дублікатів потоку даних. Така схема гарантує, що IDS залишається неперервним спостерігачем.

Системи виявлення вторгнень (IDS) бувають різних форм, включаючи систему виявлення мережевих вторгнень (NIDS), систему виявлення вторгнень на основі хоста (HIDS), систему виявлення вторгнень на основі протоколу (PIDS), систему виявлення вторгнень на основі прикладного протоколу (APIDS) та гібридну. Існує також підгрупа методів виявлення IDS. Двома найпоширенішими варіаціями є IDS на основі сигнатур та IDS на основі аномалій.

Система виявлення вторгнень (IDS) розрізняє звичайні мережеві операції та аномальні, потенційно шкідливі дії. Вона досягає цього шляхом оцінки трафіку на основі відомих моделей неправильного використання та незвичайної поведінки, зосереджуючись на невідповідностях між мережевими протоколами та поведінкою програм.

Системи запобігання вторгненням (IPS) – це динамічні рішення безпеки, які перехоплюють та аналізують шкідливий трафік. Вони діють превентивно, щоб зменшити загрози, перш ніж ті зможуть проникнути крізь мережевий захист. Це зменшує навантаження на команди безпеки.

Рисунок 2.8 – Робота системи запобігання вторгнень

Інструменти IPS особливо ефективні для виявлення та припинення спроб використання вразливостей. Вони швидко діють, щоб блокувати ці загрози, часто усуваючи розрив між появою вразливості та розгортанням патчу. З розвитком мережевої безпеки функціональність IPS інтегрується в ширші системи, такі як уніфіковані пристрої управління загрозами та брандмауери наступного покоління. Сучасні інструменти IPS також поширюються на хмарні сервіси.

Розташування IPS відбувається на прямому шляху мережевого трафіку. Це дозволяє IPS ретельно перевіряти загрози та реагувати на них у режимі реального часу, на відміну від пасивного підходу моніторингу, який використовувався її попередником, системою виявлення вторгнень (IDS). Зазвичай розташована одразу за брандмауером, IPS аналізує вхідні дані та за необхідності вживає автоматизованих дій. Системи IPS можуть сигналізувати про сповіщення, відкидати шкідливі дані, блокувати вихідні адреси та скидати з'єднання, щоб запобігти подальшим атакам.

Щоб мінімізувати хибно позитивні результати, системи запобігання вторгненням розрізняють справжні загрози та нешкідливі дані. Системи запобігання вторгненням досягають цього за допомогою різних методів, включаючи виявлення на основі сигнатур, яке спирається на відомі шаблони експлойтів; виявлення на основі аномалій, яке порівнює мережеву активність із встановленими базовими рівнями; та виявлення на основі політик, яке

забезпечує дотримання певних правил безпеки, налаштованих адміністраторами. Ці методи гарантують, що дозволено лише авторизований доступ.

Брандмауери ефективно виконують свою роль з мінімальним впливом на продуктивність мережі. Системи IDS відстежують трафік у дублікатному потоці, тому вони не порушують робочий процес мережі. Натомість, системи IPS можуть мати суттєвіший вплив на продуктивність мережі. Це пов'язано з їх вбудованим позиціонуванням та активними механізмами запобігання загрозам. Однак важливо зазначити, що сучасний дизайн інтернет-провайдерів мінімізує цей вплив.

Брандмауери, системи виявлення вторгнень та системи захисту від несанкціонованого доступу – це критично важливі компоненти мережевої безпеки, призначені для захисту інформаційних систем від загроз та несанкціонованого доступу. Кожна технологія відіграє певну роль у визначенні та управлінні потоком пакетів даних, щоб забезпечити передачу лише безпечного та легітимного трафіку, що сприяє загальній стратегії захисту цифрових активів організації.

Співпраця між цими системами підвищує безпеку. Брандмауер фільтрує початковий трафік, тоді як IDS та IPS аналізують відфільтрований трафік на наявність потенційних загроз. Такий багаторівневий підхід гарантує, що навіть якщо загроза обійде брандмауер, IDS може попередити адміністраторів про підозрілу активність, а IPS може вжити заходів, щоб запобігти заподіянню шкоди цією загрозою. Така інтеграція забезпечує більш надійну систему безпеки, здатну реагувати на широкий спектр інцидентів безпеки.

Нещодавні розробки в галузі мережевої безпеки призвели до об'єднання цих інструментів в уніфіковані рішення. Брандмауери наступного покоління поєднують функціональність традиційних брандмауерів з можливостями IDS та IPS, створюючи єдину, ефективнішу точку забезпечення дотримання політик. Ці уніфіковані системи спрощують

інфраструктуру безпеки та можуть застосовувати політики на основі комплексних даних, включаючи ідентифікацію користувача, що дозволяє здійснювати більш тонкий контроль безпеки[5].

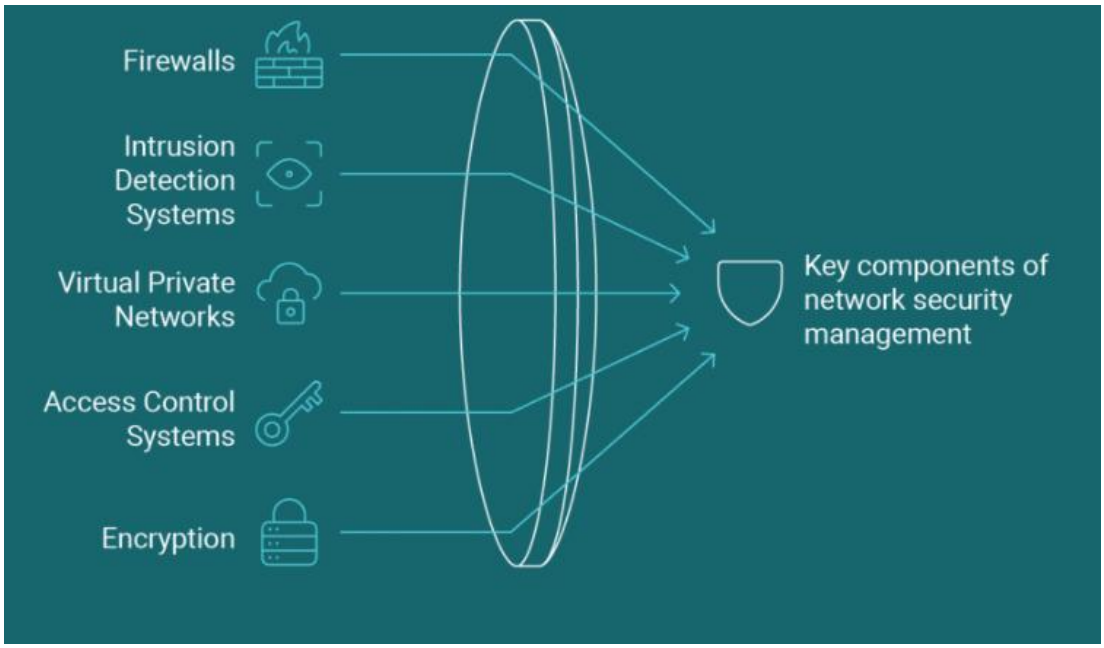

Рисунок 2.9 – Схема мережевої безпеки

Проведення регулярних аудитів безпеки шляхом систематичного огляду мережевих систем та виявлення вразливостей, а також дотримання встановлених стандартів безпеки є обов'язковим. Цей процес включає оцінку конфігурацій апаратного та програмного забезпечення, засобів контролю доступу та політик організації.

Оцінка ризиків доповнює такі аудити у виявленні потенційних загроз та оцінці їхньої ймовірності та впливу. Саме за допомогою цих процесів організації ефективно працюють над покращенням заходів безпеки.

Впровадження політик надійних паролів необхідне для запобігання несанкціонованому доступу до систем і даних. Щоб пароль вважався надійним, він повинен містити комбінацію великих і малих літер, цифр і спеціальних символів.

Хоча загальновідомо, наскільки важливо, щоб паролі були складнішими, вони все ще залишаються поширеною вразливістю та досить часто використовуються в кібератаках. Двофакторна автентифікація (2FA)

забезпечує додатковий рівень безпеки. Цей процес вимагає від користувачів підтвердження своєї особи після введення пароля за допомогою коду, надісланого на їхній телефон, або іншим подібним способом[13].

2.5 Антивірусні платформи та захист кінцевих пристроїв

Безпека кінцевих точок – це процес захисту таких пристроїв, як робочі станції, сервери та інші пристрої (які можуть приймати клієнтські програми безпеки), від зловмисних загроз та кібератак. Програмне забезпечення для безпеки кінцевих точок дозволяє компаніям захищати пристрої, які співробітники використовують для роботи, або сервери, що знаходяться в мережі або в хмарі, від кіберзагроз.

Сучасний бізнес стикається зі зростанням обсягу кіберзагроз з боку дедалі витонченіших кіберзлочинців. Хакери здійснюють кібератаки кожні 39 секунд, а щодня фіксується 2244 атаки. Кінцеві точки є однією з найпоширеніших цілей, враховуючи їхню величезну кількість, що використовується для підключення до мереж. Згідно з даними Strategy Analytics , у 2018 році вже було підключено 22 мільярди пристроїв, і, за прогнозами, до 2025 року ця цифра зросте до 38,6 мільярда пристроїв, а до 2030 року – до 50 мільярдів пристроїв. Як наслідок, у звіті Verizon про загрози було виявлено, що до 30% випадків витоку даних пов'язані з встановленням шкідливого програмного забезпечення на кінцевих точках.

Кожна кінцева точка, що підключається до корпоративної мережі, є вразливістю, що створює потенційну точку входу для кіберзлочинців. Тому кожен пристрій, який співробітник використовує для підключення до будь-якої бізнес-системи чи ресурсу, ризикує стати обраним шляхом для злому організації. Ці пристрої можуть бути використані шкідливим програмним забезпеченням, яке може призвести до витоку або красти конфіденційні дані з бізнесу.

З огляду на це, для бізнесу вкрай важливо впроваджувати рішення, які можуть аналізувати, виявляти, а потім блокувати та стримувати кібератаки в міру їх виникнення. Організаціям також необхідно співпрацювати одна з одною та використовувати технології, які забезпечують їхні IT-командам та командам безпеки видимість передових загроз, що дозволяє їм швидко виявляти ризики безпеці для швидкого усунення потенційних проблем.

Кожен пристрій, який співробітники використовують для підключення до бізнес-мереж, становить потенційний ризик, який кіберзлочинці можуть використати для крадіжки корпоративних даних. Ці пристрої, або кінцеві точки, поширюються, що ускладнює завдання їх захисту. Тому для підприємств життєво важливо впроваджувати інструменти та рішення, що захищають їхню передову лінію кібербезпеки.

Рішення для захисту кінцевих точок надає системним адміністраторам централізовану консоль керування, встановлену в мережі або на сервері, яка дозволяє їм контролювати безпеку всіх пристроїв, що підключаються до них. Потім клієнтське програмне забезпечення розгортається на кожній кінцевій точці, віддалено або безпосередньо. Після налаштування кінцевої точки програмне забезпечення надсилає на неї оновлення за потреби, автентифікує спроби входу, що здійснюються з неї, та адмініструє корпоративні політики. Крім того, рішення для захисту кінцевих точок захищає кінцеві точки за допомогою контролю програм. Це блокує завантаження або доступ користувача до програм, які є небезпечними або неавторизованими організацією. Воно також використовує шифрування для запобігання втраті даних.

Кінцеву точку можна розглядати як пристрій, який дозволяє співробітнику підключатися до корпоративної мережі. Зростання BYOD та інших підключених систем, таких як Інтернет речей (IoT), призводить до експоненціального зростання кількості пристроїв, які потенційно можуть підключатися до мережі. Деякі з найпоширеніших пристроїв, які можна вважати кінцевою точкою, включають: банкомати, розумні пристрої з

підтримкою Інтернету, промислові пристрої, ноутбуки, медичні прилади, мобільні телефони, принтери, сервери, розумні годинники.

Кінцеві точки зараз виходять за рамки ноутбуків та мобільних телефонів, які співробітники використовують для виконання своєї роботи.

Вони охоплюють будь-яку машину або підключений пристрій, який може підключитися до корпоративної мережі. І ці кінцеві точки є особливо вигідними точками входу до бізнес-мереж і систем для хакерів. Тому для організацій життєво важливо враховувати кожен пристрій, який підключений або може бути підключений до їхньої мережі, та забезпечувати його захист. Крім того, з розвитком та підвищенням складності кінцевих точок, розвиваються й рішення безпеки, які захищають їх від злому.

Антивірусне програмне забезпечення допомагає компаніям виявляти, усувати та запобігати зараженню пристроїв шкідливим програмним забезпеченням. Антивірусні рішення встановлюються безпосередньо на кінцеві пристрої, такі як ноутбуки, ПК, мережеві сервери та мобільні пристрої. Ці рішення виявляють шкідливе програмне забезпечення, скануючи файли та каталоги, щоб виявити шаблони, що відповідають визначенням та сигнатурам вірусу. Вони також можуть розпізнавати лише відомі загрози та повинні бути оновлені для виявлення найновіших штамів шкідливого програмного забезпечення[6].

Платформи захисту кінцевих точок (EPP) є важливими для захисту робочих станцій, мобільних пристроїв, серверів вашої організації. Сучасні рішення для захисту кінцевих точок включають передові превентивні заходи, такі як антивірус наступного покоління, який може блокувати як відомі, так і невідомі шкідливі програми, а також активні захисні заходи, відомі як виявлення та реагування на кінцеві точки (EDR).

NGAV доповнює традиційний антивірус на основі сигнатур поведінковим аналізом, який може виявляти нові та невідомі загрози. Він допомагає захистити мережі від шкідливого програмного забезпечення

нулевого дня, безфайлового шкідливого програмного забезпечення, програм-вимагачів та інших складних загроз.

Розглянемо найкращі програми захисту кінцевих точок.

Cynet 360 AutoXDR антивірус наступного покоління (NGAV), який блокує шкідливе програмне забезпечення, експлойти, макроси, шкідливі скрипти та інші шкідливі загрози. Захист «нульового дня» за допомогою аналітики поведінки користувачів та сутностей для виявлення та блокування підозрілої активності. Управління активами, оцінка вразливостей кінцевих точок та контроль програм, а також аудит, ведення журналу та моніторинг. Технологія обману заманює зловмисників до «приманки», збираючи корисну інформацію про методи атаки. Мережева аналітика виявляє горизонтальні переміщення, підозрілі з'єднання та входи в систему.

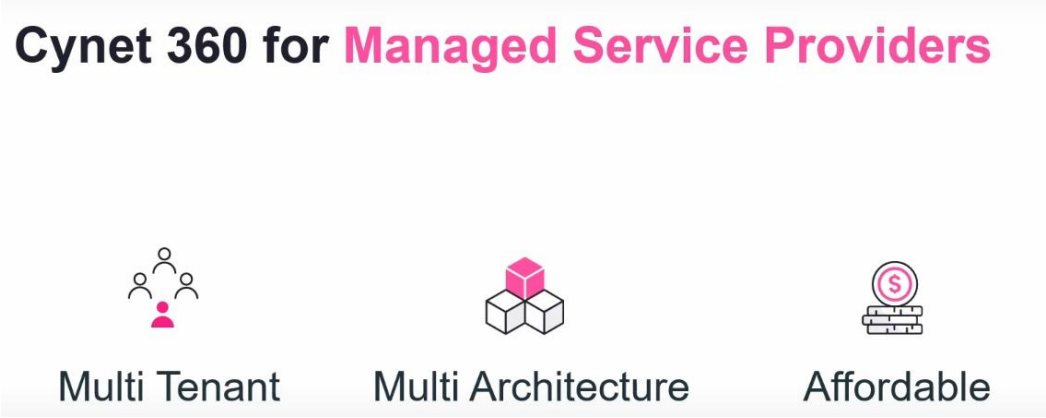

Рисунок 2.10 – Функції антивірусу Cynet

Рисунок 2.11 – Інтерфейс Cynet

Захист кінцевих точок Symantec. Функції запобігання: антивірус, брандмауер та запобігання вторгненням, контроль програм і пристроїв, включаючи доступ до файлів, реєстру та пристроїв, додавання програм до білого та чорного списків, автоматичне видалення пристроїв, забезпечення дотримання політики на хостах, блокування системи. Функції EDR: Symantec Endpoint Protection пропонує цільову аналітику атак з локальною та глобальною телеметрією, аналізом поведінки пристроїв за допомогою машинного навчання, розвідкою загроз. Допомагає в розслідуванні, стримуванні та вирішенні проблем атак.

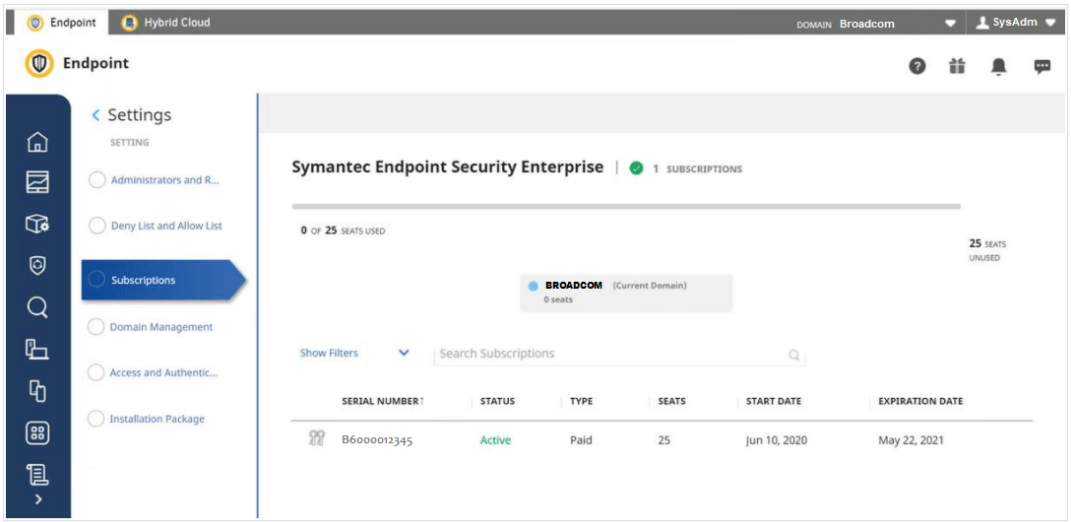

Рисунок 2.12 – Інтерфейс Symantec

Захисник Microsoft для кінцевих точок. Функції запобігання: Вбудоване керування вразливостями з можливостями виправлення. Зменшення поверхні атаки шляхом забезпечення безпечної конфігурації та застосування методів зменшення експлойтів, антивірусний захист наступного покоління для нових загроз. Можливості автоматичного розслідування, що зменшують обсяг сповіщень. Microsoft Secure Score for Devices допомагає визначити стан безпеки всієї мережі та ідентифікувати незахищені системи. Функції EDR: датчики поведінки кінцевих точок, вбудовані у Windows 10, збирають та обробляють поведінкові сигнали з операційної системи та надсилають їх до приватного хмарного екземпляра Defender for Endpoint. Рішення використовує великі дані, навчання пристроїв та унікальні метрики з усіх продуктів Microsoft та онлайн-активів, перетворюючи поведінкові сигнали на виявлення та рекомендовані відповіді. Інтегрує загрози від Microsoft та партнерів з обробки даних. Включає керовану службу пошуку загроз, яка забезпечує проактивне пошук та визначення пріоритетів для виявлення та реагування на складні загрози[7].

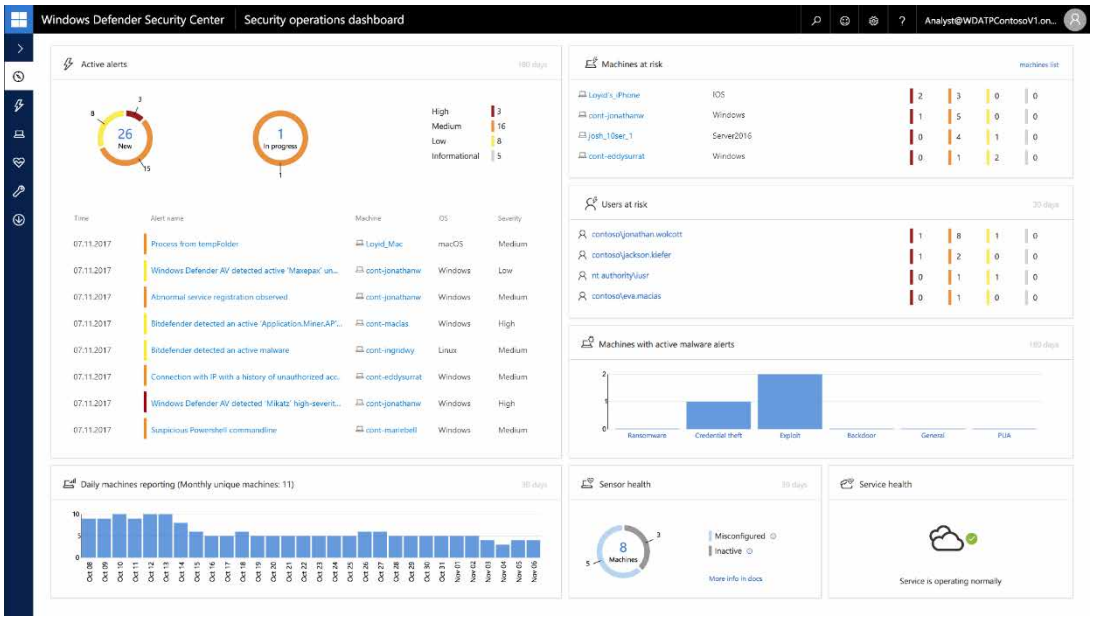

Рисунок 2.13 – Microsoft Defender

Навіть з усіма цими можливостями, жодна платформа захисту кінцевих точок не може гарантувати 100-відсоткову ефективність. Саме тому традиційне антивірусне рішення не може забезпечити достатній захист кінцевих точок. Справжнє рішення для захисту кінцевих точок наступного покоління поєднує можливості платформи захисту кінцевих точок з можливостями EDR.

2.6 Моніторинг безпеки

Ефективно виявляти, розслідувати та реагувати на загрози безпеці непросто. SIEM може допомогти.

SIEM — це технологія кібербезпеки, яка забезпечує єдине, оптимізоване уявлення про ваші дані, розуміння діяльності з безпеки та операційних можливостей, щоб ви могли випереджати кіберзагрози. Скорочення від «Security Information and Event Management» («Управління інформацією та подіями безпеки»), рішення SIEM може посилити вашу кібербезпеку, забезпечуючи повну видимість у режимі реального часу всього вашого розподіленого середовища , а також аналіз історичних даних. Технологія SIEM також може підвищити стійкість організації. Щоб виявляти загрози та інші аномалії, SIEM за лічені секунди збирає та прочісує великий обсяг даних, щоб знайти незвичайну поведінку та попередити про неї — завдання, яке інакше було б неможливо виконати вручну. Інструмент SIEM може надати знімок вашої IT-інфраструктури в будь-який момент часу. Ця здатність аналізувати дані з усіх джерел у режимі реального часу, включаючи мережеві програми, апаратне забезпечення, хмарні та SaaS-

рішення, може бути критично важливою для того, щоб допомогти організаціям випереджати внутрішні та зовнішні загрози.

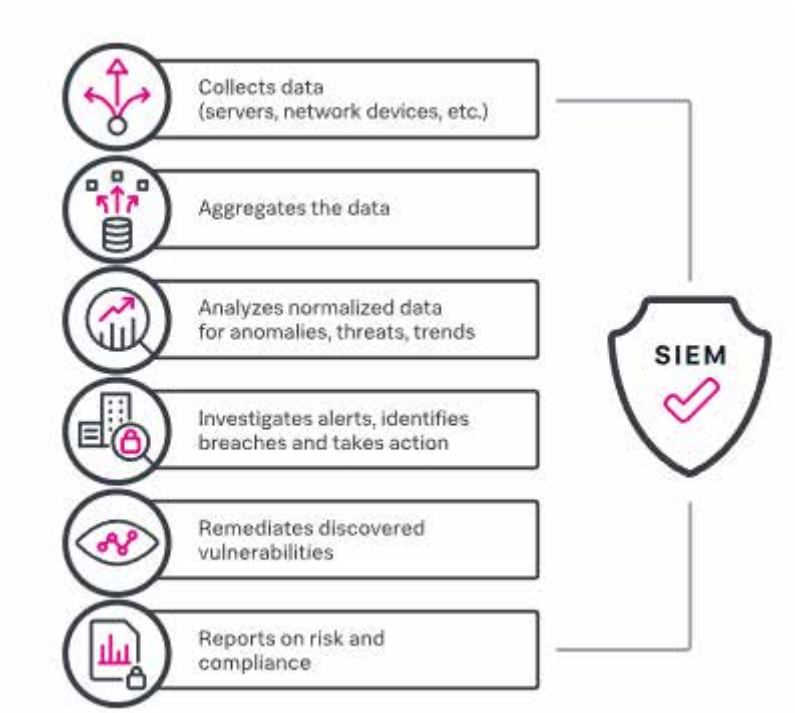

Рисунок 2.14 – Функції SIEM

Рішення SIEM агрегує дані про події з різних джерел у вашій мережевій інфраструктурі, включаючи сервери, системи, пристрої та програми, від периметра до кінцевого користувача. Зрештою, SIEM-рішення пропонує централізоване уявлення з додатковими аналітичними даними, що поєднує контекстну інформацію про ваших користувачів, активи тощо. Воно консолідує та аналізує дані на предмет відхилень від правил поведінки, визначених вашою організацією, щоб виявити потенційні загрози.

Продукти SIEM класифікуватимуть відхилення , наприклад, як «невдале входження», «зміна облікового запису» або «потенційне шкідливе

програмне забезпечення». Відхилення змушує систему сповіщати аналітиків безпеки та/або вживати заходів для призупинення незвичайної активності. Ви встановлюєте правила щодо того, що запускає сповіщення, та процедури реагування на підозрювану шкідливу активність.

Рішення SIEM також виявляє закономірності та аномальну поведінку . Таким чином, якщо одна подія сама по собі не викликає тривоги, SIEM може зрештою виявити кореляцію між кількома подіями, які в іншому випадку залишилися б непоміченими, що призведе до спрацювання сповіщення.

Перехід до хмарних обчислень призвів до розробки хмарних SIEM-рішень, які пропонують кілька переваг порівняно з традиційними локальними системами:

- масштабованість: хмарні SIEM-системи можна легко масштабувати для врахування зростаючих обсягів даних, що робить їх придатними для організацій будь-якого розміру.
- гнучкість та доступність: будучи хмарними, ці SIEM-системи забезпечують доступ з будь-якого місця, що спрощує віддалений моніторинг та керування подіями безпеки.
- економічно ефективність: вони зменшують потребу в значних початкових інвестиціях в обладнання та обслуговування, працюючи за моделлю на основі підписки, яка може бути більш економічною.
- інтеграція з хмарними сервісами: хмарні SIEM-системи розроблені для безперешкодної інтеграції з різними хмарними платформами та сервісами, забезпечуючи комплексний моніторинг безпеки в різних середовищах.

Ваш інструмент SIEM – це, по суті, командний центр безпеки, керований аналітикою, часто він є центральним елементом високофункціонального SOC. Усі дані про події збираються в централізованому місці. Інструмент SIEM виконує аналіз та категоризацію за вас. Що ще важливіше, він надає реальний контекст про події безпеки у вашій інфраструктурі[8].

Перейдемо до прикладів ПЗ SIEM.

SentinelOne пропонує надійне, уніфіковане рішення для моніторингу кібербезпеки для сучасних організацій, які прагнуть захистити всю свою цифрову інфраструктуру від постійно мінливих кіберзагроз. Платформа кінцевих точок Singularity від SentinelOne революціонізує безпеку кінцевих точок, інтегруючи виявлення загроз на основі штучного інтелекту та автономне реагування. Завдяки моніторингу активності кінцевих точок у режимі реального часу вона може автономно виявляти та нейтралізувати такі загрози, як шкідливе програмне забезпечення та програми-вимагачі, забезпечуючи мінімальні порушення роботи бізнесу. Вона використовує передові алгоритми машинного навчання для проактивної ізоляції та зменшення ризиків, покращуючи загальне управління безпекою кінцевих точок. Команди безпеки отримують користь від єдиної панелі інструментів, яка агрегує дані моніторингу, забезпечуючи повну видимість стану справ кінцевих точок та потенційних загроз. Платформа виявлення загроз SentinelOne на базі штучного інтелекту допомагає організаціям проактивно виявляти загрози та реагувати на них, перш ніж вони завдадуть шкоди.

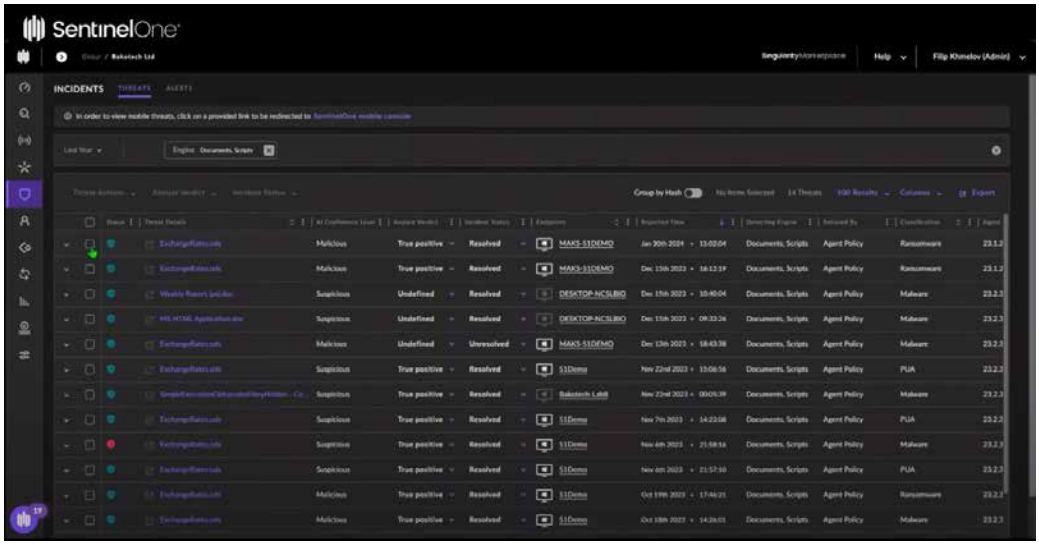

Рисунок 2.15 – Інтерфейс SentinelOne

Впровадження ефективної кібербезпеки є критично важливим для будь-якої організації, яка прагне орієнтуватися в постійно мінливому цифровому середовищі сьогодні. Вони повинні відповідати складності сучасних кібератак за допомогою проактивної стратегії кібербезпеки. Завдяки передовим інструментам моніторингу, таким як SentinelOne, організації можуть захистити свої конфіденційні дані та забезпечити безперервність своїх бізнес-операцій[9].

3 РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ МЕРЕЖІ

3.1 Вибір технологій для адміністрування захищеними мережами

Для будування захищеної мережі буду використовувати за основу топологію зірка, вона є популярною завдяки своїй простоті та надійності. Усі пристрої підключаються до центрального комутатора, що спрощує управління мережею. Вона дозволяє легко виявляти й ізолювати несправності, а також швидко додавати нові пристрої без порушення роботи всієї мережі. Така структура підходить для більшості корпоративних середовищ.

Для серверної частини буду використовувати комутатор Cisco CBS350-24T-4G.

Таблиця 3.1 – Технічні характеристики Cisco CBS350-24T-4G

Тип	Керований (Fully Managed), Layer 3 Lite
Порти доступу	24 × 10/100/1000 Mbps RJ-45 (Gigabit Ethernet)
Uplink-порти	4 × 1G SFP (оптичні порти)
Маршрутизація між VLAN (L3)	(Static Routing, VLAN Interface Routing)
Пропускна здатність (Switching)	56 Gbps

Продуктивність (Forwarding)	41.66 Mpps
Підтримка VLAN	до 4094 VLAN (IEEE 802.1Q)
Безпека	Port Security, ACL, 802.1X, DHCP Snooping, IP Source Guard, DoS Prevention
QoS (якість обслуговування)	4 черги на порт, DSCP, 802.1p, QoS ACL
Керування	Web GUI, CLI (Telnet/SSH), SNMPv3, RMON, HTTP/HTTPS

Рисунок 3.1 – Комутатор Cisco CBS350-24T-4G

Для інших груп комп'ютерів буду використовувати 2 комутатора Cisco Business CBS250-24T-4G.

Таблиця 3.2 – Технічні характеристики Cisco Business CBS250-24T-4G

Тип	Керований (Smart Managed), Layer 2+
Порти доступу	24 × 10/100/1000 Mbps RJ-45 (Gigabit Ethernet)
Uplink-порти	4 × 1G SFP (оптичні порти)

Маршрутизація між VLAN (L3)	Обмежене (Static routing, тільки між VLAN)
Пропускна здатність (Switching)	56 Gbps
Продуктивність (Forwarding)	41.66 Mpps
Підтримка VLAN	до 4094 VLAN (IEEE 802.1Q)
Безпека	Port Security, 802.1X, DHCP Snooping, DoS Protection, Access Control Lists
QoS (якість обслуговування)	4 черги на порт, DSCP, 802.1p, Rate Limiting
Керування	Web GUI, SNMPv3, CLI (через Telnet/SSH, але спрощене), RMON

Рисунок 3.2 – Комутатор CBS250-24T-4G

Маршрутизатор буду використовувати Cisco RV340, котрий ідеально підходить для захищеної мережі своїми вбудованими функціями безпеки.

Таблиця 3.3 – Технічні характеристики Cisco RV340

Тип пристрою	Gigabit VPN Router
Процесор	Dual-Core, 1.2 GHz
Оперативна пам’ять (RAM)	512 MB
Пам’ять для зберігання (Flash)	256 MB
Порти WAN	2 x RJ-45 Gigabit Ethernet (підтримка

	Dual WAN / Load Balancing / Failover)
Порти LAN	4 x RJ-45 Gigabit Ethernet
Кількість одночасних VPN тунелів	До 50 IPsec тунелів, до 10 SSL VPN
Фаервол	SPI (Stateful Packet Inspection), DoS Protection, URL Filtering
Підтримка VLAN	802.1Q, до 16 VLANs
WEB-інтерфейс	Графічний веб-інтерфейс (GUI), підтримка CLI через Telnet/SSH

Рисунок 3.3 – Маршрутизатор Cisco RV340

Для ефективного адміністрування корпоративної мережі з підвищеним ступенем захисту потрібно використовувати сучасні технології, що забезпечують логічну ізоляцію, безпечний доступ, шифрування та моніторинг. Одним із базових рішень є VLAN (Virtual Local Area Network) — технологія віртуальних локальних мереж, яка дозволяє розділити фізичну мережу на декілька логічних сегментів. Це забезпечує ізоляцію між різними групами користувачів (наприклад, адміністрація, серверна зона, бухгалтерська зона) та мінімізує ризики поширення атак у випадку компрометації одного сегмента.

Для захисту мережевого трафіку буду використовувати протокол SSH, який забезпечує шифрування всього трафіку між адміністратором та мережевим пристроєм, зокрема під час автентифікації, передавання команд і даних. SSH використовує криптографічні алгоритми для захисту

конфіденційності та цілісності інформації. Одним із основних методів автентифікації в SSH є асиметричне шифрування з використанням RSA-ключів (Rivest–Shamir–Adleman).

Для моделювання мережі я використовую RSA-ключ розміром 512 біт, що є мінімальним для активації SSH на пристрої Cisco. Проте для реального застосування в корпоративних мережах рекомендовано використовувати ключі розміром не менше 2048 біт, оскільки це забезпечує вищий рівень криптографічної стійкості згідно з сучасними стандартами безпеки. Використання сильних криптографічних ключів у поєднанні з протоколом SSH є обов'язковим елементом захисту інфраструктури корпоративної мережі від несанкціонованого доступу та перехоплення даних.

Для правильної передачі VLAN-міток між комутаторами потрібно налаштовувати транкування інтерфейсу (trunking). Режим trunk дозволяє одному порту передавати трафік з декількох VLAN, що критично важливо при побудові ієрархічної мережевої моделі. Водночас інтерфейси, котрі під'єднуються до звичайних кінцевих пристроїв переводяться в режим доступу (Access Mode) — що гарантує приналежність порту до одного конкретного VLAN і збільшує керованість мережі.

Окрему увагу слід приділяти бездротовому сегменту. Під час налаштування маршрутизатора для Wi-Fi-з'єднання доцільно застосовувати WPA2 як протокол безпеки з AES-шифруванням. Це забезпечує високий рівень захисту від несанкціонованого доступу до мережі, оскільки AES вважається одним із найнадійніших алгоритмів симетричного шифрування.

Буду використовувати ACL (Access Control Lists) — для контролю трафіку між сегментами. На обладнанні Cisco комутатори CBS250-24T-4G та CBS350-24T-4G, маршрутизатор Cisco RV340, віртуальні локальні мережі (VLAN) дозволяють розділити корпоративну мережу на ізольовані логічні сегменти, щоб мінімізувати обсяг доступних ресурсів для кожної групи користувачів і обмежити розповсюдження трафіку.

VPN — для захищеного віддаленого доступу до внутрішніх ресурсів.

SIEM-системи — для збору, аналізу та реагування на інциденти безпеки в реальному часі.

Також двофакторну автентифікацію (2FA) для захисту критично важливих систем.

Комплексне застосування вказаних технологій дозволяє побудувати багаторівневу, масштабовану та стійку до атак мережу, яка відповідає сучасним вимогам кібербезпеки.

3.2 Моделювання системи в Cisco Packet Tracer

Cisco Packet Tracer — це комплексний програмний інструмент для моделювання мереж, призначений для навчання та навчання створенню мережевих топологій та імітації сучасних комп'ютерних мереж. Інструмент пропонує унікальне поєднання реалістичного моделювання та візуалізації, можливостей оцінювання та створення завдань, а також можливостей для багатокористувацької співпраці та змагань. Його інноваційні функції допомагають учням та вчителям співпрацювати, вирішувати проблеми та вивчати концепції мереж у захопливому та динамічному соціальному середовищі[10].

Ця програма подходит для нашої мети роботи – симуляція побудови мережі та перевірка роботи комп'ютерної системи,

Ми розглянули багато засобів захисту інформації. Для реалізації моєї корпоративної мережі були використані приклади роботи та налаштування VLAN та маршрутизатора.

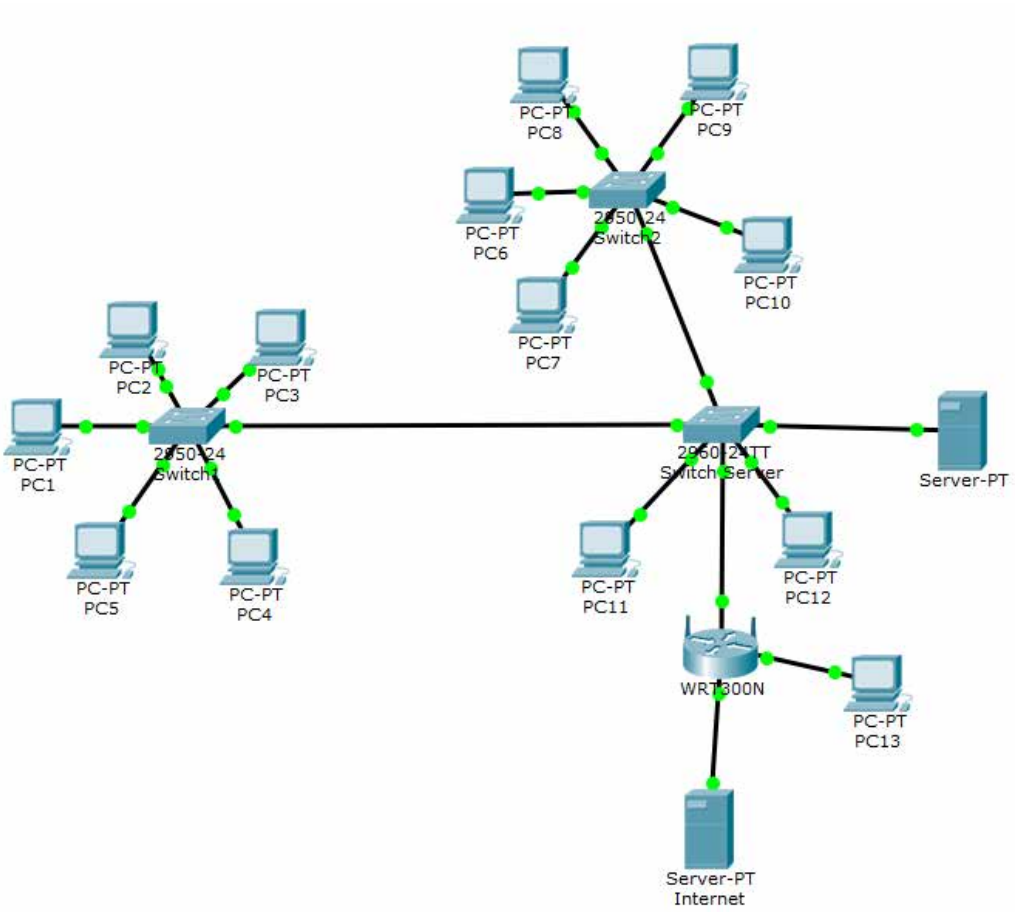

Рисунок 3.4 – Схема віртуальної мережі у Cisco Paket Tracer

Спочатку вимикаємо відповідь на DNS-запити, щоб у разі введення некоректної інформації чи команди, пристрій не сприймав її як доменне ім’я та не здійснював запит до DNS-сервера. Далі здійснюється підключення адміністративного комп’ютера до серверного комутатора з використанням протоколу SSH. Виконуємо базове налаштування комутатора: встановлюємо ім’я sw-arm, доменне ім’я admin, створюється обліковий запис користувача із паролем 123123. Робимо підвищення рівня безпеки за допомогою другої версії протоколу SSH та зробили генерування RSA-ключа з розміром на 512 біт. Активувавши режим глобальної конфігурації задається обмеження, згідно з яким віртуальні термінальні лінії (VTY) використовують виключно протокол SSH для підключення. Після цього створюється VLAN 1 для якого вписуємо IP-адресу 192.168.99.1 з маскою підмережі 255.255.255.0. Наприкінці усі зміни зберігаю до конфігурації пристрою.

```
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 123123
sw-arm(config)#enable password 123123
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]
```

Рисунок 3.5 – Основні налаштування комутатора (Switch Server)

```
sw-arm(config)#line vty 0 4
*??? 1 0:4:20.459:  RSA key size needs to be at least 768 bits for ssh version 2
*??? 1 0:4:20.459:  %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 1
sw-arm(config-vlan)#name control

sw-arm(config-vlan)#int VLAN 1
sw-arm(config-if)#
sw-arm(config-if)#ip address 192.168.99.1 255.255.255.0
sw-arm(config-if)#no sh

sw-arm(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

sw-arm(config-if)#exit
sw-arm(config)#do wr
Building configuration...
[OK]
```

Рисунок 3.6 – Створення VLAN (Switch Server)

На наступному етапі необхідно виконати транкування інтерфейса комутатора. Ця процедура дозволяє передавати трафік VLAN через одне фізичне з'єднання між мережевими пристроями. Налаштування здійснюється в режимі конфігурації на рис. 3.7, де спочатку визначається інтерфейс, який буде використовуватись як транковий, налаштовуємо параметри транкування, після чого комутатор може передавати трафік VLAN між пристроями. Таким чином, обраний інтерфейс починає функціонувати в

транковому режимі. Таку саму конфігурацію потрібно виконати й на інших комутаторах мережі, щоб забезпечити коректну взаємодію між VLAN.

```
sw-arm#en
sw-arm#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
sw-arm(config)#int fa0/1
sw-arm(config-if)#switchport mode trunk

sw-arm(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

Рисунок 3.7 – Транкування серверного комутатора (Switch Server)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname sw-arm
sw-arm(config)#vlan 2

sw-arm(config-vlan)#name control0
sw-arm(config-vlan)#int fa 0/6
sw-arm(config-if)#switchport mode trunk

sw-arm(config-if)#switchport trunk native vlan 2
sw-arm(config-if)#exit
sw-arm(config)#do wr
Building configuration...
[OK]
```

Рисунок 3.8 – Транкування звичайного комутатора (Switch1,2)

Також використовую режим доступу (Access mode) для підключення кінцевих пристроїв, таких як комп’ютери, принтери та інші робочі станції, на рис. 3.9 схематично зображено принцип підключення робочої станції до комутатора. В параметрах спочатку задаю діапазон інтерфейсів, які використовуватимуться для підключення. Після цього кожному інтерфейсу присвоюється відповідний номер, щоб забезпечити правильне сортування трафіку в межах віртуальної мережі.

```
sw-arm(config)#vlan 3
sw-arm(config-vlan)#name controll

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 4

sw-arm(config-if-range)#exit
sw-arm(config)#do wr
Building configuration...
[OK]
```

Рисунок 3.9 – Створення групи VLAN та включення Access mode

Далі налаштовуємо бездоротовий маршрутизатор, який є дуже важливим елементом в захищеній мережі. У початковій конфігурації використовується статична IP-адреса 10.10.0.3 з маскою підмережі 255.255.255.248. У ролі шлюзу вказано IP-адресу інтерфейсу FastEthernet 0/0, який налаштований на комутаторі серверної частини мережі. Наступний етап конфігурації передбачає призначення IP-адрес співробітникам та клієнтам на рис. 3.11. Вказуємо адрес DNS-сервера, який необхідний для коректного з'єднання поштового сервера з мережею.

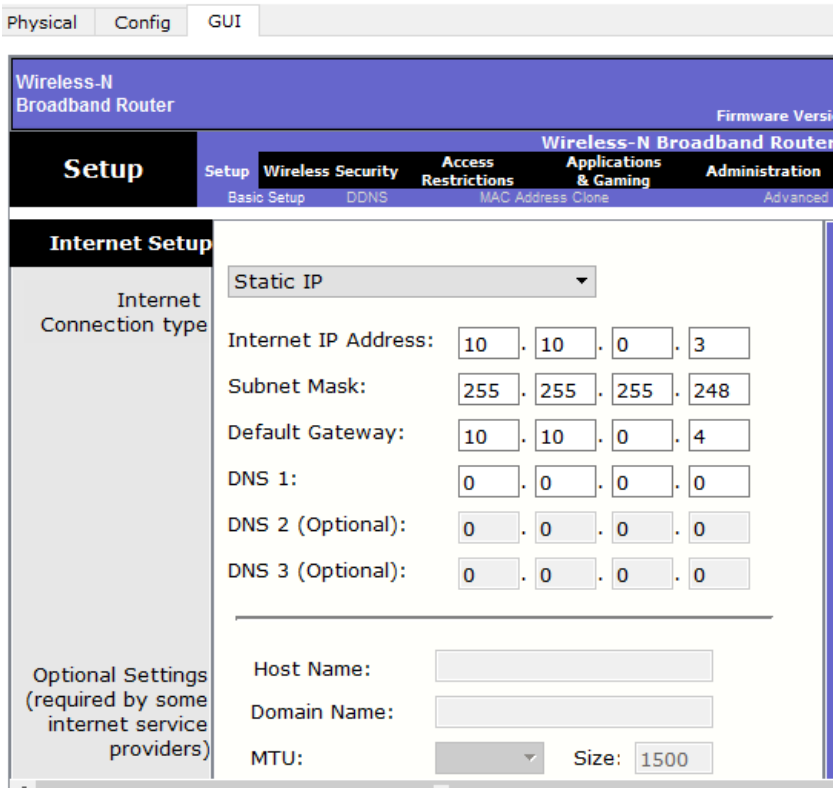

Рисунок 3.10 – Налаштування IP-адресу

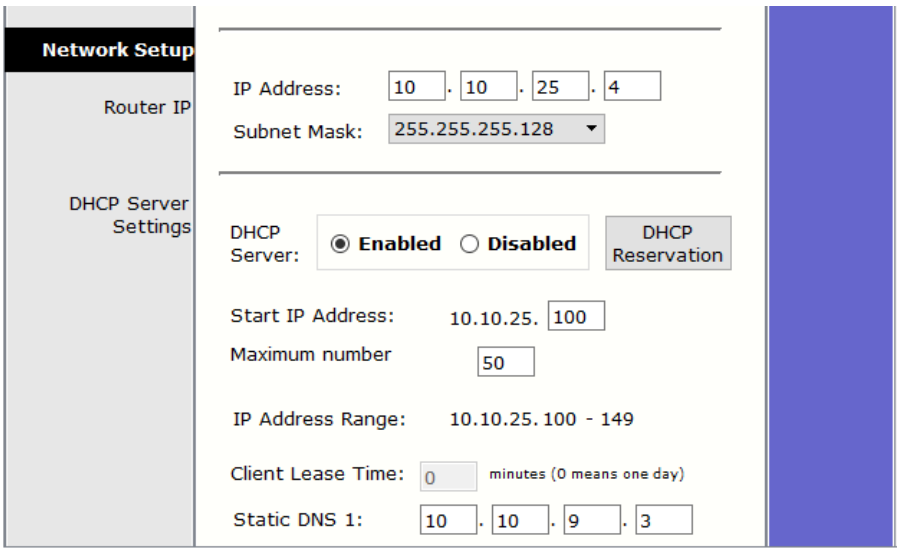

Рисунок 3.11 – Налаштування роздачі IP-адресу персоналу

У вкладці Wireless було створено бездротову мережу з ім’ям admin1. На цьому етапі доступні додаткові параметри, зокрема для активації ширококанального режиму, але стандартні налаштування підходять. Далі, для забезпечення захисту мережі, було відкрито вкладку Wireless Security, де з доступних варіантів протоколів безпеки було обрано WPA2 із використанням алгоритму шифрування AES. Також було встановлено пароль FDhj&74hD для підключення до мережі на рис. 3.13.

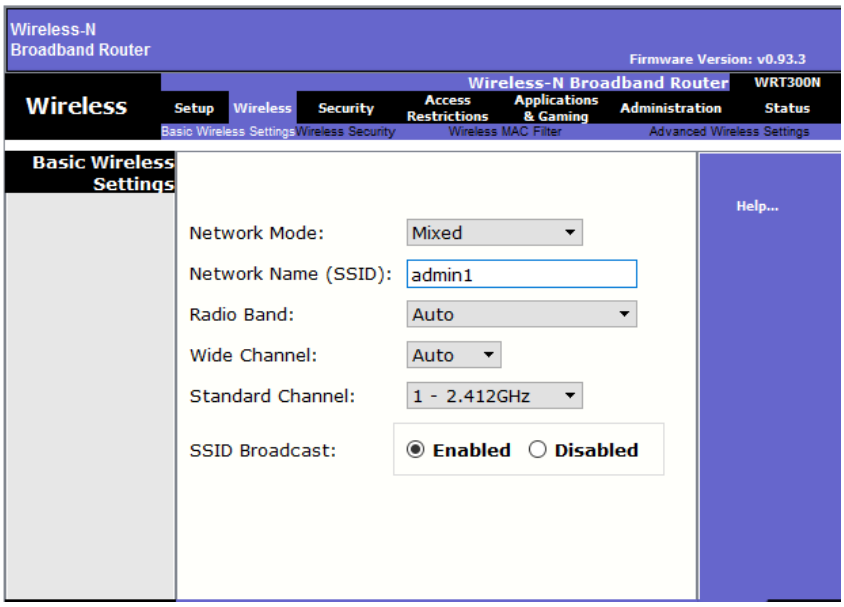

Рисунок 3.12 – Налаштування маршрутизатора

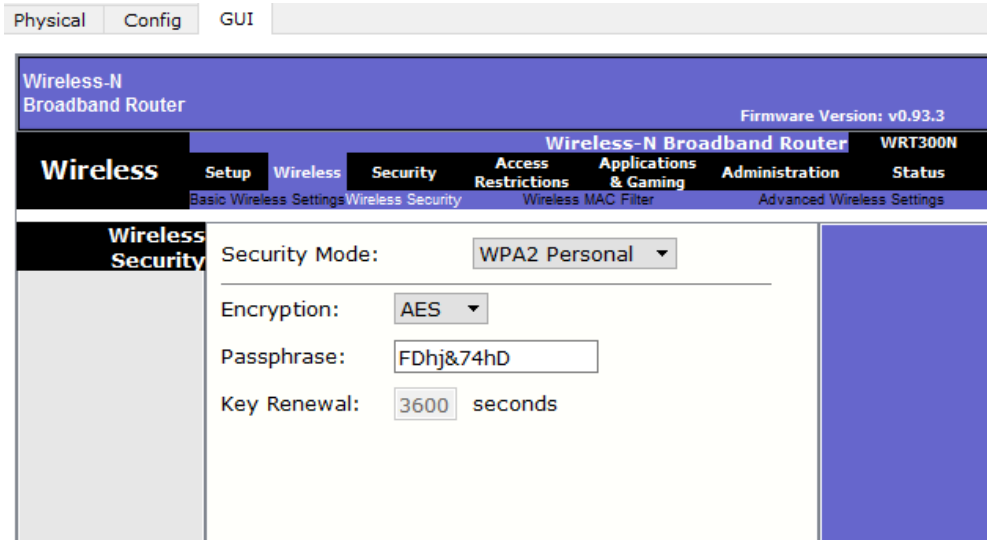

Рисунок 3.13 – Налаштування роздачі IP-адресу персоналу

3.3 Рекомендації для адміністрування захищеними мережами

Адміністрування захищених мереж потребує комплексного підходу, котрий охоплює як технічні засоби оборони, так і організаційні заходи. Завданням мого проекту є забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів у корпоративному середовищі. Далі я наведу ключові рекомендації, котрі слід враховувати при створенні та обслуговуванні безпечної мережевої інфраструктури.

Рекомендую використовувати сегментацію мережі. Розділення мережі на логічні сегменти за допомогою VLAN дозволяє зменшити ризики поширення шкідливого трафіку та обмежити доступ між окремими відділами. Нариклад, у компанії створено VLAN 10 для бухгалтерії, VLAN 20 для продажів і VLAN 30 для адміністрації. Між VLAN діє політика фільтрації за допомогою ACL, яка дозволяє лише необхідні з’єднання, наприклад, доступ бухгалтерії до серверу баз даних.

Використовувати протокол 802.1X з сервером RADIUS, який дозволяє реалізувати автентифікацію на рівні порту. Це означає, що пристрій не зможе отримати доступ до мережі без перевірки облікових даних користувача. Наприклад, ноутбук працівника організації не отримає IP-адресу або доступ

до корпоративної мережі, поки користувач не введе логін і пароль, що перевіряється на RADIUS-сервері.

Для захищеного віддаленого доступу обов'язковим є використання VPN-з'єднання (IPsec або SSL). Це гарантує шифрування переданих даних і захист від прослуховування. Наприклад, адміністратор підключається до корпоративної мережі через маршрутизатор Cisco RV340 за допомогою IPsec VPN-тунелю. Трафік шифрується, і доступ можливий лише після автентифікації за сертифікатом.

Фаєрволи фільтрують трафік відповідно до політик безпеки. Потрібно налаштувати обмежувальні правила за замовчуванням (default deny) та дозволяти лише необхідні з'єднання. Наприклад, на Cisco RV340 налаштовано правило: дозволити доступ до веб-сервера тільки з IP-адрес діапазону 192.168.10.0/24, всі інші з'єднання — блокуються.

Періодичне оновлення прошивок комутаторів, маршрутизаторів та іншого обладнання дозволяє уникати відомих вразливостей. Оновлення потрібно проводити лише з офіційних джерел. Комутатор Cisco CBS350 автоматично повідомляє про наявність нової прошивки через веб-інтерфейс. Адміністратор завантажує її з сайту Cisco та виконує оновлення в контрольованому середовищі.

Впровадження систем логування (наприклад, Syslog, SNMP, NetFlow) дозволяє фіксувати події в мережі, що критично для виявлення загроз і розслідування інцидентів. Cisco комутатори надсилають журнали подій на сервер логів. У разі виявлення підозрілої активності — багаторазової зміни MAC-адрес на одному порту — адміністратор отримує сповіщення.

Навіть із найкращим мережевим захистом уразливість може виникнути через недбало налаштований комп'ютер. Кінцеві пристрої повинні мати антивірусне ПЗ з актуальними базами, шифрування диску (наприклад, BitLocker), контроль USB-портів, актуальні оновлення. Наприклад, на всіх робочих станціях працівників увімкнено Windows Defender, шифрування

BitLocker, а доступ до USB-накопичувачів обмежено через групові політики (GPO).

Людський фактор — головна загроза. Необхідно проводити тренінги для персоналу з тем:

- як розпізнавати фішингові листи;

- як працювати з VPN;

- чому не варто використовувати один пароль всюди;

Захист корпоративної мережі — це не окрема дія, а постійний процес, що включає проєктування архітектури, налаштування обладнання, оновлення, моніторинг, а також навчання користувачів. Лише комплексний підхід забезпечує справжню кіберстійкість.

ВИСНОВКИ

У процесі виконання дипломної роботи було досліджено, проаналізовано та реалізовано комплекс заходів, необхідних для створення, захисту та ефективного адміністрування сучасної корпоративної мережі.

На основі аналізу технічного завдання та сучасних вимог до інформаційної безпеки сформульовано ключові підходи до побудови безпечного середовища.

У першому розділі було проведено аналіз технічного завдання, вивчено поняття корпоративної мережі, її структуру, функціональні особливості та вимоги до захисту. Був зроблений вибір мережевого обладнання, комутаторів Cisco CBS250-24T-4G, CBS350-24T-4G та маршрутизатора Cisco RV340, які відповідають сучасним вимогам до безпеки та масштабованості.

У другому розділі розглянуто ключові засоби забезпечення мережевої безпеки. Проаналізовано різновиди систем захисту, зокрема фаерволи, системи контролю доступу, антивірусний захист, а також засоби криптографії, зокрема використання RSA-ключів у протоколі SSH.

Розглянуто переваги впровадження криптографічних методів у захищену взаємодію між пристроями, а також необхідність шифрування даних і автентифікації на основі сертифікатів. Значна увага приділялася моніторингу безпеки, зокрема використанню Syslog, SNMP та аналізу трафіку для виявлення аномалій.

У третьому розділі безпосередньо реалізовано проект моделювання захищеної мережі з використанням програмного середовища Cisco Packet Tracer. Була змодельована структура корпоративної мережі з впровадженням VLAN, фільтрації трафіку, контролю доступу, а також реалізовано базову політику безпеки.

Розроблено рекомендації для адміністрування захищеними системами, використання багатоетапної автентифікації, регулярного оновлення ПЗ, резервного копіювання, сегментації мережі та навчання персоналу з кібергігієни.

Результати роботи можуть бути використані як методичний приклад побудови та адміністрування захищених корпоративних мереж у малому та середньому бізнесі, а також як основа для подальших досліджень у сфері інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Горбенко В. Ф. Інформаційно-комунікаційні технології. Розділ 13. Мережеві технології [Електронний ресурс] – Режим доступу: https://kppk.com.ua/ELLIB/ebook/Gorbenko/IKT/13/13.htm
2. Городецька О. М. Інформаційна безпека комп'ютерних систем : навчальний посібник / О. М. Городецька. – Вінниця : ВНТУ, 2017. – 129 с. – [Електронний ресурс] – Режим доступу: https://pdf.lib.vntu.edu.ua/books/IRVC/2021/Gorodetska_2017_129.pdf
3. Fortinet. Access Control – Визначення та принципи [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/access-control
4. Infosec Institute. Firewalls and IDS/IPS – основи захисту мережі [Електронний ресурс] – Режим доступу: https://www.infosecinstitute.com/resources/network-security-101/firewalls-and-ids-ips/
5. Palo Alto Networks. Firewall vs IDS vs IPS [Електронний ресурс] – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/firewall-vs-ids-vs-ips
6. Fortinet. Endpoint Security – захист кінцевих пристроїв [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security
7. Cynet. Найкращі платформи захисту кінцевих точок [Електронний ресурс] – Режим доступу: https://www.cynet.com/endpoint-protection/top-6-endpoint-protection-platforms-and-how-to-choose/
8. Splunk. SIEM – Security Information and Event Management [Електронний ресурс] – Режим доступу:

https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
9. SentinelOne. Cybersecurity Monitoring – основи моніторингу безпеки [Електронний ресурс] – Режим доступу: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/
10. Cisco Networking Academy. Cisco Packet Tracer – навчальне середовище [Електронний ресурс] – Режим доступу: https://www.netacad.com/cisco-packet-tracer
11. SpectralOps. Криптографія та мережна безпека – короткий огляд [Електронний ресурс] – Режим доступу: https://spectralops.io/blog/cryptography-and-network-security-the-quick-and-short-guide/
12. Geeks for Geeks. Криптографія та її види [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/cryptography-and-its-types/
13. Potomac University. Network Security Management – управління безпекою [Електронний ресурс] – Режим доступу: https://potomac.edu/network-security-management/