МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ, ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Віктор ГНАТЮК
“_____”_____2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Кібербезпека інформаційно-комунікаційних систем»

Виконавець: _____ Дмитро КОВАЛЕНКО
(підпис)

Керівник: _____ Георгій КОНАХОВИЧ
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Катерина КАЖАН
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Лариса ЧЕРНЯК
(підпис)

Нормоконтролер: _____ Богдан ЧУМАЧЕНКО
(підпис)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет аеронавігації, електроніки та телекомунікацій .
Кафедра телекомунікаційних та радіоелектронних систем .
Спеціальність 172 «Електронні комунікації та радіотехніка» .
Освітньо-професійна програма «Телекомунікаційні системи та мережі» .

ЗАТВЕРДЖУЮ
Завідувач кафедри

Віктор ГНАТЮК
“_____”_____2025 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Коваленка Дмитра Юрійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Кібербезпека інформаційно-комунікаційних систем»

затверджена наказом ректора від «02» вересня 2025 р. № 1672 /ст

2. Термін виконання роботи: з 29.09.2025 р. по 31.12.2025 р.

3. Вихідні дані до роботи: Кібербезпека інформаційно-комунікаційних систем.

4. Зміст пояснювальної записки: 1. Дослідження структури інформаційно-комунікаційних систем і основ кібербезпеки; 2. Аналіз загроз і вразливостей сучасних інформаційно-комунікаційних систем; 3. Розгляд ключових міжнародних і національних стандартів у кібербезпеці; 4. Огляд основних методів і засобів захисту інформації; 5. Аналіз актуальних кіберзагроз; 6. Практична реалізація без-пеки корпоративної мережі за допомогою Cisco Packet Tracer.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	29.09.2025-30.09.2025	Виконано
2	Вступ	01.10.2025-03.10.2025	Виконано
3	Основи кібербезпеки інформаційно-комунікаційних систем	04.10.2025-14.10.2025	Виконано
4	Сучасні методи та засоби забезпечення кібербезпеки	15.10.2025-26.10.2025	Виконано
5	Аналіз актуальних кіберзагроз	27.10.2025-10.11.2025	Виконано
6	Дослідження методів забезпечення корпоративної ІКС	10.11.2025-16.11.2025	Виконано
7	Охорона праці	17.11.2025-30.11.2025	Виконано
8	Охорона навколишнього середовища	01.12.2025-14.12.2025	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	15.12.2025-31.12.2025	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.т.н., доц. Катерина КАЖАН		
Охорона навколишнього середовища	д.т.н., доц. Лариса ЧЕРНЯК		

8. Дата видачі завдання: «01» вересня 2025 р.

Керівник кваліфікаційної роботи _____ Георгій КОНАХОВИЧ
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Дмитро КОВАЛЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Кібербезпека інформаційно-комунікаційних систем» містить 76 сторінок, 29 рисунків, 1 таблицю, 30 використаних джерел.

КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, СТАНДАРТИ ISO/IEC 27001, NIST, GDPR, КРИПТОГРАФІЯ, IDS/IPS, SIEM, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, CISCO PACKET TRACER, КОРПОРАТИВНА МЕРЕЖА, БЕЗПЕКА VLAN, WI-FI.

Об’єкт дослідження – інформаційно-комунікаційні системи та їх захище-ність від кіберзагроз.

Предмет дослідження – методи та засоби забезпечення кібербезпеки інформаційно-комунікаційних систем.

Мета кваліфікаційної роботи – дослідження основ кібербезпеки, аналіз сучасних загроз і вразливостей, вивчен-ня методів захисту та практична реалізація заходів безпеки в корпоративній мережі.

Метод дослідження – в роботі розглядається кібербезпека з різних пози-цій: архітектури інформацій-но-комунікаційних систем, ключових міжнародних та національних стандартів (ISO/IEC 27001, NIST, GDPR), сучасних методів та засобів захисту (криптогра-фія, IDS/IPS, SIEM, MFA, PAM), а також актуальних кіберзагроз (соціальна ін-женерія, фішинг, вразливості віддаленої роботи).

Проводиться порівняльний аналіз методів забезпечення кібербезпеки. Аналізуються типові вразливості інформаційно-комунікаційних систем. Наво-диться перелік векторів атак з посиланнями на методи запобігання.

Практична частина включає розробку логічної топології локальної мережі, налаштування маршрутизації, DHCP, DNS, VLAN, безпеки Wi-Fi та тестування на вразливості в середовищі Cisco Packet Tracer.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

API (Application Programming Interface) — програмний інтерфейс, що визначає способи взаємодії між програмними компонентами або сервісами.

DHCP (Dynamic Host Configuration Protocol) — протокол динамічного призначення IP-адрес та інших параметрів мережевої конфігурації вузлам.

DNS (Domain Name System) — ієрархічна система доменних імен, що перетворює доменні імена на IP-адреси.

DoS (Denial of Service) — атака на відмову в обслуговуванні, що перешкоджає коректній роботі сервісу або мережі.

FTP (File Transfer Protocol) — протокол прикладного рівня для передавання файлів між клієнтом і сервером.

IPsec (Internet Protocol Security) — набір протоколів захисту IP-трафіку за допомогою шифрування та аутентифікації.

ISO/IEC 27001 — міжнародний стандарт, що визначає вимоги до системи менеджменту інформаційної безпеки (ISMS).

MAC (Media Access Control) — апаратна адреса мережевого інтерфейсу, що використовується на канальному рівні.

MFA (Multi-Factor Authentication) — багатофакторна аутентифікація з використанням двох і більше незалежних факторів.

NAT (Network Address Translation) — технологія трансляції приватних IP-адрес у публічні й навпаки.

NGFW (Next-Generation Firewall) — міжмережевий екран нового покоління з підтримкою аналізу трафіку на рівні застосунків і контент-фільтрації.

Nmap (Network Mapper) — інструмент для сканування мереж і виявлення відкритих портів і служб.

OPA (Open Policy Agent) — рушій політик, що дозволяє реалізувати підхід Policy-as-Code для інфраструктури та сервісів.

PAM (Privileged Access Management) — система керування привілейованим доступом до критичних ресурсів.

PGP (Pretty Good Privacy) — криптографічний протокол для захисту електронної пошти й файлів.

SQL (Structured Query Language) — мова структурованих запитів для ро-боти з реляційними базами даних.

SSH (Secure Shell) — протокол захищеного віддаленого доступу до командної оболонки й адміністрування систем.

SSL (Secure Sockets Layer) — застарілий протокол захищеного обміну да-ними, що був попередником TLS.

TLS (Transport Layer Security) — криптографічний протокол захисту транспортного рівня для веб-та інших сервісів.

UDP (User Datagram Protocol) — транспортний протокол без установлення з’єднання, що забезпечує мінімальні затримки передавання.

VLAN (Virtual Local Area Network) — віртуальна локальна мережа, що логічно сегментує мережеву інфраструктуру незалежно від фізичної топології.

VPN (Virtual Private Network) — технологія створення захищеного тунелю поверх незахищених мереж, таких як Інтернет.

ВСТУП

Актуальність теми. Світ активно використовує інформаційно-комунікаційні системи, вони обслуговують найрізноманітніші сфери - від державних установ і великих корпорацій до освітніх закладів і навіть повсякденних домашніх користувачів. Величезна кількість даних, які обробляються, та висока складність мереж роблять їх особливо вразливими до різноманітних кіберзагроз. Із розвитком технологій кіберзлочинці використовують дедалі витончені методи, тож забезпечення кібербезпеки виходить за рамки простої технічної задачі - це питання захисту, довіри, стабіль-ності і безпеки суспільства загалом.

Щоб ефективно боротися з сучасними загрозами, потрібно застосовувати комплексний підхід: впроваджувати актуальні технології, дотримуватися міжнародних стандартів і оперативно реагувати на інциденти. Особливо важливо розуміти, що кібербезпека - повинна поширюватися у всіх організаціях.

Мета і завдання дослідження. В моїй роботі проведено детальний аналіз інформаційно-комунікаційних систем, їхніх вразливостей і загроз. Робота має практичні аспекти - роботу з інструментами Packet Tracer для виявлення і реагування на кіберінциденти. Мета роботи - створення зрозумілого, детального погляду на кібербезпеку, для забезпечення безпечної, стабільної роботи інформаційних систем в цифровому середовищі.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Аналіз існуючих підходів до забезпечення кібербезпеки інформаційно-комунікаційних систем та класифікація сучасних кіберзагроз і вразливостей.
2. Дослідження архітектури корпоративних мереж, включаючи сегментацію, вико-ристання VLAN та захист бездротових мереж Wi-Fi.
3. Узагальнення міжнародних та національних стандартів і нормативних вимог у сфері кібербезпеки (зокрема, ISO/IEC 27001, NIST, GDPR) та їхнього впливу на побудову системи захисту.

4. Аналіз сучасних методів і засобів захисту (криптографія, IDS/IPS, SIEM, механізми аутентифікації, контролю доступу, MFA, PAM) та визначення їх ролі в ком-плексному забезпеченні безпеки.
5. Проєктування та моделювання захищеної корпоративної мережі в середовищі Cisco Packet Tracer із налаштуванням маршрутизації, DHCP, DNS, VLAN і Wi-Fi.
6. Проведення експериментальних досліджень стійкості мережі до типових атак (VLAN hopping, DoS/DDoS, спроби несанкціонованого доступу) та оцінка ефек-тивності запропонованих заходів захисту.

Об'єктом дослідження – це процес забезпечення кібербезпеки інформаційно-комунікаційних систем корпоративної мережі.

Предметом дослідження – це методи, засоби та організаційно-технічні рішення щодо захисту інформаційно-комунікаційних систем, зокрема застосування криптографічних механізмів, IDS/IPS, SIEM, а також технологій сегментації мережі й захисту Wi-Fi у корпо-ративному середовищі. Об'єкт і предмет дослідження є категоріями наукового процесу і співвідносяться між собою як загальне і часткове. У об'єкті виділяється та його частина, що служить предметом дослідження. Саме на нього і спря-мована основна увага випускника, саме предмет дослідження визначає тему ква-ліфікаційної роботи.

Методи досліджень. У роботі використано аналіз і синтез наукових джерел з кібербезпеки, порівня-льний аналіз стандартів і засобів захисту, методи моделювання корпоративної мережі в програмному середовищі, емпіричні методи випробувань і тестування (імітація атак, аналіз журналів подій, оцінка показників стійкості та ефективності захисту). Наукова новизна та практичне значення отриманих результатів.

Наукова новизна та практичне значення отриманих результатів.

Наукова новизна отриманих результатів:

1. Удосконалено підхід до комплексного забезпечення кібербезпеки корпоративної мережі за рахунок поєднання сегментації (VLAN, DMZ),

сучасних криптографічних протоколів, IDS/IPS та SIEM у єдиній логічній моделі.

2. Запропоновано структуровану модель оцінювання стійкості корпоративної мережі до типових мережевих атак, що враховує параметри конфігурації маршру-тизації, служби DHCP/DNS, Wi-Fi захисту та політик доступу.

Практичне значення отриманих результатів:

1. Розроблена модель корпоративної мережі та налаштовані засоби захисту можуть бути використані як типове рішення для впровадження базового комплексу кіберзахисту в організаціях малого та середнього бізнесу.
2. Запропоновані рекомендації щодо використання стандартів ISO/IEC 27001, NIST, GDPR, а також практичні налаштування мережевих сервісів і засобів за-хисту можуть бути застосовані при проєктуванні, аудиті та модернізації існую-чих інформаційно-комунікаційних систем.

РОЗДІЛ 1
ОСНОВИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

1.1. Що таке інформаційно-комунікаційні системи та класифікація

Інформаційно-комунікаційні системи (ІКС) - це сукупність апаратних, програмних та організаційних засобів, що забезпечують збір, обробку, зберігання і передачу інформації з метою підтримки процесів управління, виробництва чи надання послуг. Вони об’єднують комп’ютерні мережі, сервери, мережеве обладнання, програмне забезпечення, а також організаційні процедури, що сприяють ефективній взаємодії користувачів та інформаційних потоків. За функціональним призначенням ІКС поділяються на інформаційні, комунікаційні та аналітичні системи, за охопленням - локальні, регіональні і глобальні, за масштабом - від персональних до міжнародних, а також за типом обробки даних - централізовані, розподілені та хмарні. Також важливо виділяти звичайні системи та критичні, які підтримують безперебійне функціонування важливих сфер, таких як охорона здоров’я, фінанси чи державне управління.

Інформаційно-комунікаційні системи можна поділити на кілька основних груп залежно від їхніх функцій. Локальні інформаційно-комунікаційні системи функціонують у межах окремих підприємств чи установ, забезпечуючи внутрішні процеси управління та обробки інформації. Регіональні системи охоплюють ширші географічні області, інтегруючи декілька локальних мереж. Глобальні ж системи мають масштаб, що простягається на національний або навіть міжнародний рівень, забезпечуючи взаємодію між багатьма користувачами в різних точках світу.

Щодо масштабу, системи можуть обслуговувати індивідуальних користувачів або великі групи. Індивідуальні системи орієнтовані на потреби окремої людини, групові - на обмежений колектив, корпоративні - на організації сотень або тисяч

працівників. Національні й міжнародні системи ж служать для координації діяльності державних структур або глобальних корпорацій.

За технологією обробки даних ІКС можна поділити на централізовані, де більшість операцій виконується у одному місці; розподілені, що мають декілька вузлів обробки і зберігання інформації, розподілених територіально; і хмарні системи, які використовують ресурси Інтернету для забезпечення гнучкості та масштабованості.

Окремо виділяють системи за рівнем їх критичності. Звичайні системи підтримують щоденні операції з низьким рівнем ризику, тоді як критичні системи відповідають за функціонування інфраструктур, наприклад, охорони здоров'я, енергетики, фінансів і державного управління. Помилки чи атаки на такі ІКС можуть мати серйозні наслідки для безпеки і стабільності.

Класифікація є важливою основою для розробки належних стратегій кібербезпеки, адаптованих до конкретних типів систем та масштабів їх функціонування. Такий підхід дозволяє безпечно інтегрувати новітні технології та забезпечувати надійний захист інформацій у сучасному цифровому середовищі, врахо-вуючи різні рівні та сфери застосування.

1.2. Загрози та вразливості сучасних ІКС

ІКС постійно піддаються загрозам, які можуть призвести до порушення цілісності, конфіденційності та доступності інформації. Серед основних загроз - шкідливе програмне забезпечення, хакерські атаки, DDoS, соціальна інженерія, а також проблеми, що виникають через людський фактор чи технічні помилки.

Вразливості систем можуть полягати у старих або невчасно оновлених програмних компонентах, неправильному налаштуванні систем безпеки, відсутності сегментації мереж, а також в низькій обізнаності користувачів. Кіберзагрози у 2025 році стали більш комплексними із застосуванням штучного інтелекту, персоналізованих атак і нових методів обходу систем захисту. Ця динаміка створює

необхідність у впровадженні ефективних процедур моніторингу, реагування і управління ризиками.

1.3. Кібербезпека та її роль у системі інформаційної безпеки

Сучасний захист інформаційних ресурсів охоплює комплекс заходів, спрямованих на попередження несанкціонованого доступу, зміни, викрадення або пошкодження даних, а також забезпечення безперебійної роботи мереж і цифрових пристроїв. Він ґрунтується на трьох головних принципах: конфіденційності (захист інформації від небажаного розголошення), цілісності (забезпечення точності та незмінності даних) і доступності (гарантія доступу до ресурсів у потрібний момент). Підходи до такого захисту поєднують технічні рішення, організаційні процедури та правові рамки, що дозволяє комплексно протистояти різним видам загроз.

Значення цих заходів зросло в умовах широкої цифровізації та зростання щоденної кількості кібератак, які загрожують функціонуванню як приватних, так і державних структур. Надійний захист інформації відіграє ключову роль у формуванні довіри до цифрових сервісів, що надзвичайно важливо для бізнесу, державних установ і кінцевих користувачів. Порушення безпеки часто призводить до значних фінансових збитків, втрати репутації, а в деяких випадках — до загрози національній безпеці через можливість зламу критичних інфраструктур.

Захист інформації є складовою ширшої системи, яка також включає фізичні засоби охорони, кадрову політику, нормативно-правове регулювання та методичне забезпечення. Фізичний контроль включає обмеження доступу до технічних приміщень і серверів для запобігання несанкціонованому фізичному втручанню. Кадрові заходи спрямовані на формування обізнаності співробітників, управління правами доступу відповідно до їхніх ролей і професіоналізацію персоналу зі сфери захисту інформації. Нормативна база визначає законодавчі і галузеві стандарти, які встановлюють мінімальні вимоги до захисту даних, а методичні документи формалізують внутрішні процедури реагування на кібератаки і моніторинг стану безпеки.

Заходи безпеки поділяються на превентивні та реактивні. До першої кате-горії належать використання антивірусів, систем виявлення та запобігання втор-гнень, брандмауерів, систем шифрування і управління доступом. Реактивні дії включають постійний моніторинг інцидентів, аналіз загроз, а також швидке реа-гування для мінімізації наслідків атак і відновлення роботи систем. Інноваційні технології, зокрема штучний інтелект і машинне навчання, дедалі більше засто-совуються для виявлення складних і новітніх загроз автоматизовано, що підви-щує ефективність протидії.

Важливою складовою є взаємодія між державними органами, приватним сектором і академічною спільнотою для спільного виявлення кіберзагроз, обмі-ну інформацією та координації дій з нейтралізації потенційних інцидентів. По-шириним напрямком є також поширення принципів кібергігієни — простих пра-вил поведінки для користувачів, які допомагають значно знизити ризики кібер-загроз.

Таким чином, комплексний підхід до захисту інформації на технічному, організаційному, нормативному та соціальному рівнях є запорукою стабільності цифрових технологій і довіри до них. Його ефективність безпосередньо впливає на безпеку як окремих користувачів, так і великих корпорацій і держав.

1.4. Ключові міжнародні та національні стандарти у сфері кібербезпеки

Захист інформаційно-комунікаційних систем сьогодні неможливий без урахування загальноприйнятих стандартів, які встановлюють універсальні правила та принципи побудови стійких систем безпеки. Міжнародні стандарти допомагають організаціям різних країн впроваджувати передові методи захисту, які вже перевірені на практиці та відповідають сучасним загрозам.

Одним з найпоширеніших стандартів є ISO 27001, який описує систему управління інформаційною безпекою, що включає процеси оцінки ризиків, впровадження політик і контролю їх виконання. Це дозволяє не лише виявляти уразливості, а й регулярно покращувати системи захисту. На додаток ISO 27002

детально регламентує конкретні технічні та організаційні заходи, які покликані мінімізувати ризики.

Фінансовий сектор і компанії, що працюють із платіжними картками, повинні відповідати стандарту PCI DSS, який визначає конкретні правила шифрування, моніторингу та контролю доступу. Надійний криптографічний захист гарантує FIPS 140, що стандартизує модулі для шифрування інформації.

В Україні кібербезпека регулюється власними нормами, серед яких особливо важливими є державні стандарти серії ДСТУ 3396, що регламентують технічний захист інформації, криптографічні методи (ДСТУ 7624 і ДСТУ 7564) та електронний цифровий підпис (ДСТУ 4145). Ці стандарти допомагають сформувати надійний фундамент для безпеки у державному секторі та комерційних структурах.

У сфері кібербезпеки стандарти відіграють важливу роль, оскільки вони встановлюють вимоги до процесів, методів і засобів захисту інформації, що забезпечують узгодженість і ефективність заходів безпеки на різних рівнях організацій та секторів. Дотримання цих стандартів є передумовою для підвищення довіри користувачів, партнерів та державних органів до інформаційних систем.

ISO/IEC 27001 - це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (ISMS). Він встановлює структуру для впровадження, моніторингу, підтримки й удосконалення політики безпеки в організації. Основною метою стандарту є забезпечення конфіденційності, цілісності та доступності інформації шляхом системного підходу до управління ризиками. Впровадження ISO/IEC 27001 дозволяє організаціям ідентифікувати та ефективно управляти кіберризиками, а також відповідати законодавчим вимогам і галузевим нормам.

Фреймворк кібербезпеки від Національного інституту стандартів і технологій США (NIST) представляє собою керівництво з побудови ефективної системи кіберзахисту. Він складається з п’яти основних функцій: ідентифікація, захист, виявлення, реагування і відновлення. NIST пропонує гнучкий підхід, який може бути адаптований під особливості будь-яких організацій незалежно від їх розміру й сфери

діяльності. Використання цього фреймворку допомагає покращити готовність до кіберінцидентів і підвищити стійкість IT-інфраструктури.

Регламент Загального Захисту Даних (GDPR) Європейського Союзу є основним нормативним актом, що регламентує обробку персональних даних. Він встановлює суворі вимоги до захисту приватності громадян, зокрема, у сфері кібербезпеки, через обов'язкове впровадження технічних та організаційних заходів для забезпечення безпеки даних. GDPR суттєво впливає на інформаційно-комунікаційні системи, що працюють з персональними даними, змушуючи їх адаптувати процеси згідно із встановленими стандартами захисту інформації.

Впровадження таких стандартів дає змогу організаціям не лише дотримуватися вимог законодавства, а й підтримувати високий рівень захищеності, що формує довіру клієнтів, партнерів і суспільства в цілому. Стандарти - це своєрідний каркас, навколо якого формується вся система кібербезпеки, що захищає дані і сервіси від сучасних кіберзагроз.

Таким чином, стандарти відіграють роль маяка, який допомагає організаціям орієнтуватися у складному світі кіберзагроз, запроваджуючи перевірені правила і методи, адаптовані під сучасні виклики. Лише поєднання стандартів із передовими технологіями і людським фактором дозволяє побудувати надійний захист інформаційно-комунікаційних систем.

1.5. Фаєрвол та конфігурація мережі

Фаєрвол (брандмауер, міжмережевий екран) є одним із базових засобів мережевої безпеки, призначеним для контролю та фільтрації трафіку між різними сегментами мережі на основі наперед визначених правил доступу. Його основна роль полягає у створенні бар'єру між довіреним середовищем (локальна мережа організації) та недовіреним середовищем (зовнішні мережі, зокрема Інтернет), а також між окремими внутрішніми сегментами, які мають різний рівень довіри. Фаєрвол аналізує параметри мережевих пакетів (IP-адреси джерела та призначення, порти, протоколи, напрямок з'єднання) і приймає рішення про дозвіл або заборону

проходження трафіку, що дозволяє зменшити ризик несанкціонованого доступу, поширення шкідливого ПЗ та мережевих атак.

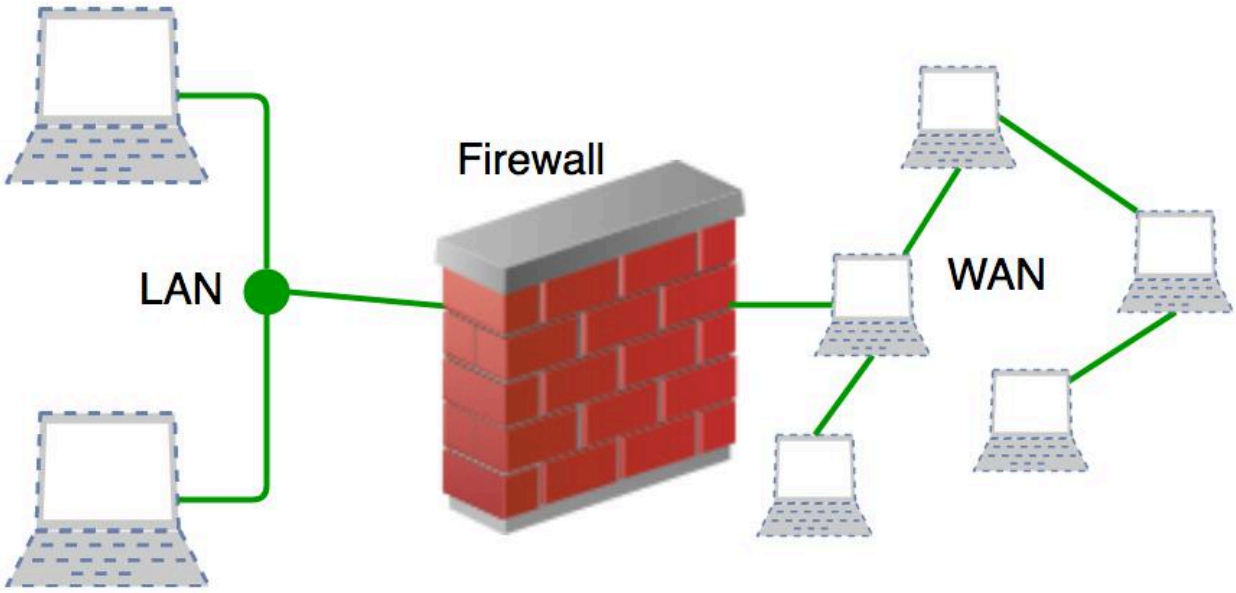

Рис. 1.1. Ілюстрація роботи Фаєрволу

З погляду мережевої архітектури, фаєрвол є ключовим елементом сегментації, тобто логічного поділу корпоративної мережі на окремі зони безпеки. Типовий приклад - виділення внутрішньої зони (internal network), демілітаризованої зони (DMZ) для розміщення публічних сервісів (веб-, поштові, FTP-сервери) та зовнішньої зони (Internet). Між цими зонами налаштовуються різні рівні довіри: внутрішня мережа вважається більш захищеною, а зовнішня – найбільш ризикованою. Фаєрвол реалізує політику «мінімальних привілеїв», згідно з якою за замовчуванням трафік між зонами блокується, а дозволи надаються лише для чітко визначених сервісів і напрямків. Це особливо важливо для протидії поширеним загрозам, таким як сканування портів, експлуатація вразливостей сервісів та розповсюдження шкідливих програмних компонентів.

За принципом роботи розрізняють кілька типів фаєрволів. Фаєрволи фільтрації пакетів здійснюють аналіз лише заголовків пакетів і приймають рішення на основі IP-адрес, протоколів і портів. Stateful-фаєрволи здійснюють контроль стану з’єднань: вони відстежують, які сесії ініційовані з внутрішньої мережі, та пропускають лише

легальні відповіді, що підвищує захист від спроб встановлення небажаних з'єднань ззовні. Фаєрволи прикладного рівня (application-level) аналізують вміст трафіку, працюючи на рівні конкретних протоколів (HTTP, SMTP тощо) і дають змогу фільтрувати шкідливі запити, наприклад SQL-ін'єкції чи XSS-атаки. Сучасні міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW) поєднують традиційні механізми фільтрації з поглибленим аналізом трафіку, виявленням вторгнень, контролем застосунків та іноді функціями антивірусу.

Важливою складовою є інтеграція фаєрволу з іншими елементами мережевої інфраструктури. У типових корпоративних мережах фаєрвол розміщують на межі з Інтернетом, а також між критичними внутрішніми сегментами з різними рівнями доступу (наприклад, користувацькі станції, серверний сегмент, гостьова мережа). Такий підхід дозволяє реалізувати зоновану модель безпеки, коли порушення в одній зоні не призводить до автоматичної компрометації всієї мережі. Крім того, журнали подій фаєрволу можуть передаватися до систем централізованого моніторингу та аналізу безпеки (SIEM), що забезпечує кореляцію подій, виявлення аномалій і формування більш повної картини інцидентів у мережі.

Таким чином, фаєрвол є невід'ємною частиною багаторівневої системи кібербезпеки, яка доповнює інші засоби захисту (IDS/IPS, антивірус, криптографічні протоколи, механізми автентифікації) та забезпечує реалізацію політик доступу на мережевому рівні. Грамотно спроєктована мережева конфігурація фаєрволу дає змогу суттєво знизити ризики, пов'язані з сучасними кіберзагрозами, та підвищити стійкість інформаційно-комунікаційних систем до атак.

1.6. Безпека Wi-Fi мереж

Wi-Fi технології забезпечують мобільність і гнучкість доступу до інформаційних ресурсів, але водночас створюють додаткові вектори атак, оскільки радіоканал доступний для перехоплення будь-яким користувачем у зоні покриття. Основними загрозами для бездротових мереж є несанкціонований доступ, перехоплення трафіку (атаки типу «людина посередині» - MITM), підбір слабких

паролів, створення фальшивих точок доступу (evil twin), а також використання вразливостей застарілих протоколів шифрування. У корпоративному середовищі компрометація Wi-Fi може призвести до несанкціонованого доступу до критичних внутрішніх ресурсів, витоку конфіденційних даних і подолання інших захисних механізмів.

Ключовим захисним механізмом Wi-Fi є застосування криптографічних протоколів, які забезпечують шифрування трафіку й контроль цілісності переданих даних. Історично використовувався протокол WEP, який на сьогодні вважається небезпечним через наявність відомих криптоаналітичних атак. Його змінили більш захищені протоколи WPA та WPA2, що базуються на використанні алгоритму AES у режимах CCMP для досягнення конфіденційності й цілісності. Останнім етапом розвитку є стандарт WPA3, який впроваджує більш стійкі механізми обміну ключами та захист від офлайн-підбору паролів, підвищуючи рівень безпеки особливо в публічних і корпоративних мережах.

У корпоративних мережах рекомендується застосовувати режим WPA2-Enterprise або WPA3-Enterprise з використанням протоколу 802.1X та сервера RADIUS для автентифікації користувачів. На відміну від Pre-Shared Key (PSK), де всі користувачі поділяють один пароль, Enterprise-режим дає змогу призначати унікальні облікові дані кожному суб’єкту доступу. Це полегшує керування правами, відкликання доступу, а також аудит дій користувачів. Поєднання 802.1X з багатофакторною автентифікацією значно знижує ризики, пов’язані з компрометацією паролів і соціальною інженерією, та узгоджується з сучасними підходами до побудови безпечних інформаційних систем.

Важливим аспектом є логічна сегментація бездротової мережі. Різні категорії користувачів (персонал, гості, технічні служби) мають отримувати доступ до окремих мереж, які ізольовані одна від одної за допомогою механізмів VLAN та правил доступу. Наприклад, гостьова мережа повинна мати обмежений доступ лише до Інтернету, без виходу до внутрішніх серверів та критичних сервісів. Такий поділ доповнюється налаштуванням фаєрволу, який контролює взаємодію між сегментами та запобігає горизонтальному розповсюдженню атак у разі компрометації одного з

них. Цей підхід відповідає принципам зонної безпеки та мінімізації наслідків інцидентів.

Окрему увагу слід приділяти додатковим заходам захисту Wi-Fi: відключенню небезпечних або застарілих функцій (зокрема WPS), застосуванню складних і унікальних паролів, регулярній зміні ключів доступу, фільтрації за MAC-адресами (як допоміжному заходу), а також своєчасному оновленню прошивки точок доступу. Важливим є також моніторинг бездротового середовища за допомогою засобів виявлення вторгнень (IDS/IPS), здатних фіксувати підозрілу активність, появу неавторизованих точок доступу та аномалії в трафіку. Інформація про події Wi-Fi може інтегруватися в системи централізованого моніторингу безпеки для глибшого аналізу інцидентів і формування адекватних заходів реагування.

ВИСНОВКИ ДО РОЗДІЛУ 1

Проведено аналіз інформаційно-комунікаційних систем, актуальних кіберзагроз і типових вразливостей, включно з особливостями побудови корпоративних мереж, сегментації, використанням DMZ та захисту Wi-Fi. На основі огляду сучасних стандартів і підходів окреслено базові вимоги до безпечної архітектури мережі, що стала підґрунтям для подальшого проєктування та впровадження засобів захисту.

РОЗДІЛ 2
СУЧАСНІ МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

2.1. Шифрування та криптографічні методи захисту інформації

Криптографічні методи захисту інформації представляють собою набір спеціальних технік, що включають шифрування, кодування та інші способи перетворення даних, які роблять інформацію недоступною для несанкціонованих осіб без наявності відповідного ключа. Основна мета криптографії - гарантувати конфіденційність, цілісність і автентичність даних, забезпечуючи максимальний захист інформації від злому, підробки чи несанкціонованого доступу.

Сучасна криптографія поділяє методи захисту на симетричні та асиметричні. У першому випадку для шифрування і дешифрування використовується однаковий секретний ключ, що забезпечує швидке й ефективне перетворення великих обсягів даних. Найпоширенішим алгоритмом є AES, який широко застосовується у державних, фінансових та комерційних системах. Асиметричні методи базуються на парі ключів - відкритому, публічно доступному для шифрування, та закритому, який використовують для дешифрування. Цей підхід особливо важливий для передачі даних через відкриті канали та створення електронних підписів, що підтверджують достовірність інформації. Алгоритми RSA і еліптичної криптографії є лідерами в цій категорії.

Крім основних методів шифрування, велике значення мають інструменти, які гарантують цілісність даних. Хеш-функції генерують унікальні цифрові «відбитки», які змінюються навіть при незначній зміні вмісту повідомлення. Ці відбитки дозволяють виявити будь-які підробки або випадкові помилки. Коди автентифікації повідомлень поєднують хешування і криптографію, що дає змогу підтвердити справжність відправника та зберегти незмінність інформації. Електронний цифровий підпис виконує роль особистого підпису в електронному світі і є ключовим елементом у правовідносинах і офіційному документообігу.

У широкому обсязі криптографічні методи вбудовані в різні протоколи захисту інформації. Наприклад, протоколи SSL і TLS забезпечують безпечний доступ до вебресурсів, захищаючи передані дані від перехоплення та підробки.

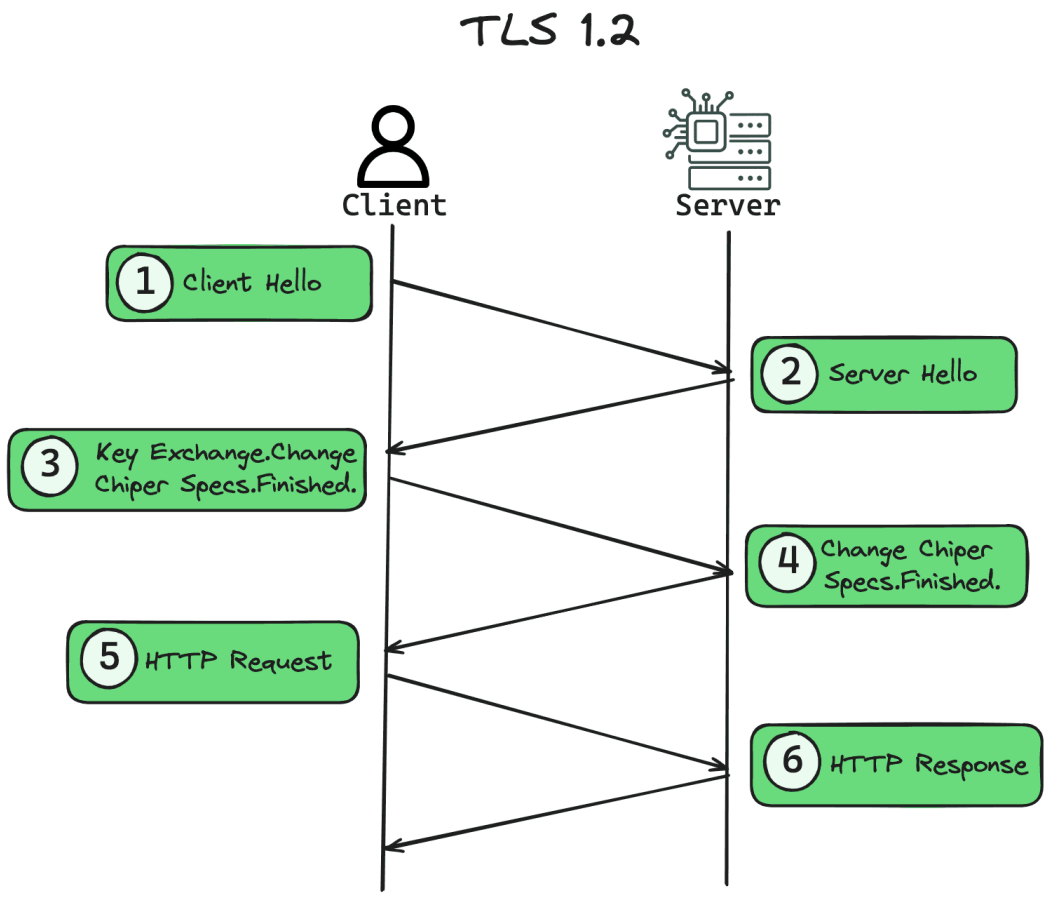

Рис. 2.1. Принцип роботи Transport layer Security

IPsec гарантує безпеку мережевого рівня, захищаючи обмін інформацією у корпоративних мережах і VPN. Електронна пошта шифрується за допомогою PGP або S/MIME, що допомагає уникнути втручання у приватне спілкування.

В Україні особливу увагу приділяють впровадженню національних стандартів, такими як ДСТУ «Калина» та «Купина», що забезпечують надійний криптографічний захист і застосовуються у державних інформаційних системах і важливих бізнес-процесах. Впровадження таких стандартів гарантує сумісність і відповідність національним і міжнародним вимогам.

Вже сьогодні активно розвивається квантова криптографія — технологія, що обіцяє революційний рівень безпеки завдяки використанню фундаментальних властивостей квантових частинок. Вона дозволяє передавати ключі абсолютно надійно, оскільки будь-яке втручання відразу виявляється. Хоча її повсюдне впровадження ще на початковій стадії, потенціал для майбутнього безпечного цифрового світу великий.

Практичне застосування криптографії включає організацію зашифрованих каналів зв’язку для забезпечення безпеки мережевого трафіку, використання цифрових підписів для юридично значущої аутентифікації документів і безпечне зберігання інформації, що допомагає уникнути витоків конфіденційних даних.

Таким чином, криптографічні методи є незамінним інструментом сучасної кібербезпеки. Вони дозволяють перетворювати інформацію в таку форму, яка захищена від несанкціонованого доступу, забезпечує її цілісність та довіру користувачів. Організації, що впроваджують сучасні криптографічні рішення, набагато краще готові протистояти швидкозмінним загрозам цифрової епохи, підтримуючи довгострокову безпеку та стабільність своєї діяльності.

2.2. Приклади систем автентифікації та керування доступом

Системи автентифікації і керування доступом у 2025 році стали справжніми «щитами» в цифровому світі, котрі не лише захищають інформацію, а й роблять користування сервісами зручнішим і швидшим. Автентифікація - це впевненість у тому, що користувач, який заходить у систему, дійсно той, за кого себе видає. У житті це схоже на момент, коли вас при вході просять пред'явити посвідчення особи. У світі цифрових технологій цей процес набув різних форм і став багатогранним.

Використання паролів досі є найбільш розповсюдженим способом захисту, але ні для кого не секрет, що просто пароль вже недостатньо. Зловмисники все частіше використовують складні схеми злому паролів, а люди часто вибирають прості або повторно використовують їх у різних сервісах. Саме тому багатофакторна автентифікація стала нормою сучасного захисту: це коли, щоб підтвердити свою

особу, потрібно не лише знати пароль, а й мати доступ до мобільного телефону, отримати код із спеціального додатку, або навіть пройти біометричну перевірку.

Біометрія - це справжня революція в автентифікації. Вона базується на унікальних фізіологічних або поведінкових характеристиках людини, такі як відбитки пальців, розпізнавання обличчя, голосу або навіть малюнок вен. Біометричні системи вже не є чимось з наукової фантастики — вони допомагають нам розблокувати смартфони, підтвердити особу при оплатах чи авторизуватися в державних сервісах. Ключова перевага біометрії - складність фальсифікації, що значно підвищує рівень захисту.

Керування доступом сьогодні часто реалізується через спеціалізовані системи, що дозволяють централізовано контролювати, які користувачі та якими правами володіють. Завдяки цим системам кожен працівник має доступ лише до тих ресурсів, які йому потрібні для роботи, а всі дії користувачів ретельно відстежуються. Такі рішення допомагають зменшити ризики недобросовісного використання даних і відповідати вимогам законодавства щодо захисту персональних даних.

Однією з важливих функцій сучасних систем є єдиний вхід, який дозволяє користувачам авторизуватися один раз і отримати доступ до всіх необхідних сервісів без повторного введення паролів. Це позбавляє від необхідності запам’ятовувати численні паролі, знижує ризики помилок і робить роботу користувача значно комфортнішою.

Для адміністраторів і працівників з підвищеними правами існують спеціальні системи управління привілейованим доступом, які забезпечують додатковий рівень контролю та моніторингу. Вони допомагають запобігти внутрішнім загрозам і зловживанням, фіксуючи кожен крок користувача і автоматично блокуючи доступ у разі підозрілої активності.

Хмарні технології врізноманітнили і розширили можливості автентифікації та контролю доступу. Зараз користувач може працювати в офісі чи вдома, з будь-якого куточка світу, а хмарні платформи автоматично підлаштовують рівень безпеки й доступу відповідно до ролей, пристроїв і локації. Це особливо важливо для сучасних компаній із гнучкими режимами роботи і розподіленими командами.

Гармонійне поєднання технологій, таких як багатофакторна автентифікація, біометричний контроль, централізоване управління ролями й автоматичний аудит, формують надійну базу безпеки. Вони дають змогу людям і організаціям не лише захищати свої дані, але й робити це з комфортом, не витрачаючи зайвий час, що є вагомим фактором у цифровому світі.

Таким чином, сучасні системи автентифікації та керування доступом не просто оберігають наші цифрові активи. Вони створюють довіру, забезпечують оперативність і роблять світ інформаційних технологій більш відкритим і безпечним для кожного з нас.

2.3. Робота IDS/IPS і SIEM

Системи IDS, IPS і SIEM відіграють особливу роль у побудові надійного захисту інформаційних мереж і ресурсів. IDS (система виявлення вторгнень) служить пасивним спостерігачем, що займається моніторингом мережевого трафіку та виявленням підозрілої активності або порушень політик безпеки. Вона не втручається у роботу мережі, а лише повідомляє адміністраторів про потенційні загрози. IDS може бути як мережевою, так і хостовою, виявляючи як атакувальний трафік, так і внутрішні порушення.

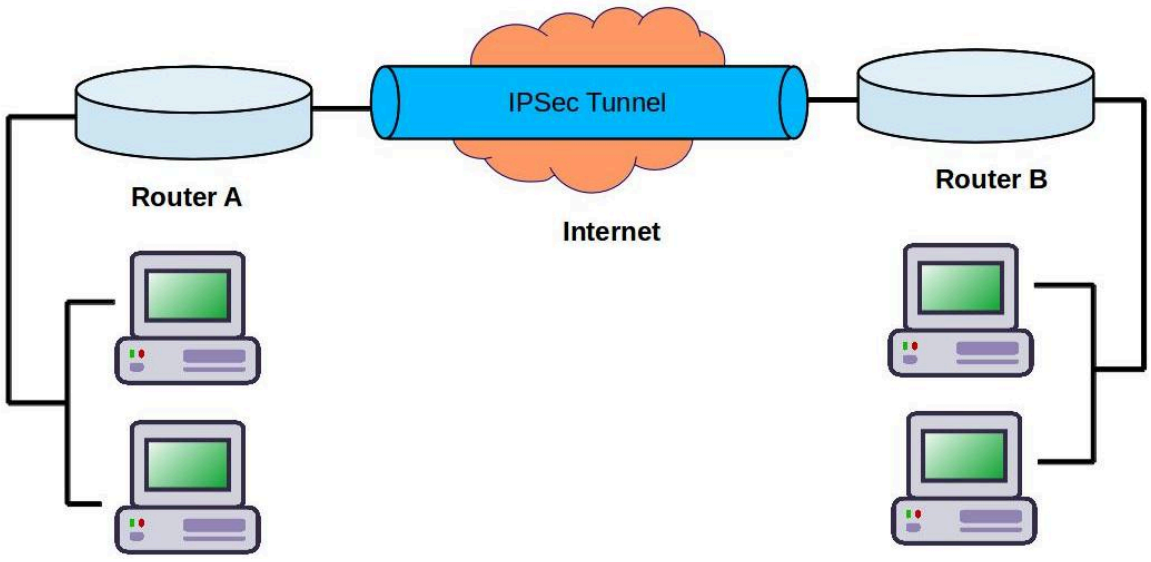

Рис. 2.2. Принцип роботи IPS

IPS (система запобігання вторгненням) є активною системою, яка здатна не тільки розпізнавати загрози, а й одразу блокувати небезпечний трафік чи дії у мережі. Вона працює в реальному часі і запобігає реалізації атак, наприклад, скидаючи з'єднання зі злочинним сервером чи обмежуючи доступ порушника.

SIEM (система управління інформацією та подіями безпеки) - це централізований інструмент, що збирає, аналізує та корелює дані походження різних джерел - від IDS/IPS, файрволів, серверів, додатків до мережевого обладнання. SIEM дозволяє побачити загальну картину безпеки, виділити актуальні загрози, автоматизувати оповіщення, звітність і допомогти командам з реагування на інциденти дієво і вчасно. Вона широко застосовує штучний інтелект і аналітику поведінки користувачів для точного виявлення складних атак.

Ключові відмінності: IDS фіксує та сповіщає, IPS активно запобігає атакам, а SIEM агрегує велику кількість даних, аналізує і допомагає управляти безпекою в цілому. Ці системи доповнюють одна одну: наприклад, дані з IDS та IPS збираються і аналізуються в SIEM, що дозволяє підвищити ефективність виявлення та реагування.

Впровадження таких інструментів особливо актуальне для складних корпоративних мереж, банків, державних установ, де безпека критично важлива. Правильно налаштовані IDS/IPS разом із SIEM забезпечують багато рівнів захисту: від швидкого реагування на інциденти, автоматичної ізоляції атак, до глибокого аналізу ознак загроз і складання профілів атакувальників.

У результаті, ці системи створюють багатошарову оборону: IDS і IPS - це «сторожові собаки», які охороняють мережу в реальному часі, а SIEM - це «аналітичний центр», який координує всі дії, робить інформацію зрозумілішою і допомагає приймати правильні рішення для безпеки.

Цей інструментарій забезпечує як проактивний захист, так і глибокий аналіз, завдяки чому організації здатні швидко виявляти і відбивати навіть нові форми атак, підтримуючи безперервність бізнес-процесів і захищаючи критичну інформацію.

2.4. Захист на практиці

Для імітації та детального дослідження захищеності мережі в роботі було застосовано інструменти - Cisco Packet Tracer та, що дозволяють одночасно моделювати мережеву інфраструктуру і аналізувати мережевий трафік.

Початковим кроком стало моделювання корпоративної мережі в Packet Tracer із впровадженням кількох VLAN, кожна з яких асоціюється з конкретним відділом або групою співробітників. Такий розподіл дозволяє реалізувати сегментацію трафіку, що не лише покращує організацію даних усередині підприємства, а й підвищує безпеку, обмежуючи міжмережевий рух і доступ.

Packet Tracer застосовувався для моніторингу а також, щоб швидко виявляти будь-які порушення безпеки. Зокрема, аналізувався трафік на предмет з’явлення незареєстрованих MAC-адрес, повторних логінів чи підроблених пакетів, що свідчить про спроби несанкціонованого доступу або атаки. Він дозволяє ефективно фільтрувати та відстежувати аномальні події, надаючи адміністраторам мережею цінну інформацію для прийняття оперативних рішень.

Цей комплексний підхід, що поєднує точне моделювання мережі і скрупульозний аналіз трафіку, дозволяє не лише активно виявляти загрози, але й впроваджувати ефективні заходи протидії, забезпечуючи захист на всіх рівнях - від архітектури і конфігурації мережі до глибокого контролю її експлуатації.

Таким чином, реалізація захисту мереж із використанням стійких протоколів аутентифікації й сучасних інструментів моніторингу створює надійний бар’єр проти зловмисників. Методологія, застосована в роботі, демонструє, як теоретичні знання з кібербезпеки можна ефективно трансформувати у практичні навички для захисту складних корпоративних мереж.

Таке поєднання практичного моделювання, аналізу і налаштувань важливо не тільки для наукових цілей, а й для подальшої успішної роботи в галузі інформаційної безпеки. Реалізовуючи ці підходи на реальних підприємствах, можна значно знизити ризик атаки, втрати даних або простої в мережі, що є ключовим фактором для підтримки стабільної й безпечної роботи організації.

2.5. Безпека хмарних сервісів

Безпека хмарних сервісів - це не просто технічне завдання, а комплексний підхід, який поєднує технології, політики та людський фактор для захисту цінної інформації, яка зберігається і обробляється в хмарі. Хмарні сервіси сьогодні є важливою частиною інфраструктури будь-якої організації - від малих бізнесів до великих підприємств і державних установ. Вони дають змогу зручно масштабувати ресурси, працювати з будь-якої точки світу і зменшують витрати на обладнання. Водночас при цьому хмара відкриває нові вектори атаки, що вимагає продуманих і складних методів захисту.

Основи безпеки хмарних сервісів починаються зі зміцнення конфіденційності та цілісності даних. Надійне шифрування інформації перед передачею і під час зберігання є фактично «замком», який захищає дані навіть у разі порушення безпеки. Особливість хмарних технологій у тому, що обробка і зберігання відбуваються на віддалених серверах, тому важливо використовувати криптографію на боці користувача, тобто шифрувати дані до того, як вони потраплять у хмару. Це підвищує загальний рівень довіри до хмарних послуг.

Підтвердження особи користувачів та контроль за їхніми правами доступу - ключ до надійного захисту у хмарних середовищах. Багатофакторна автентифікація вже є обов’язковою практикою; вона спонукає користувача пройти кілька рівнів перевірки - від пароля до коду в мобільному додатку чи біометричних даних. Також застосовують адаптивний контроль доступу, який враховує контекст - геолокацію, пристрій, історію дій - і регулює рівень перевірки, забезпечуючи кращий баланс між безпекою і зручністю.

Моніторинг та аналіз активності в хмарі здійснюється спеціалізованими системами, серед яких SIEM посідає центральне місце. Вона збирає дані з різних джерел, аналізує аномалії, автоматично оповіщає про підозрілі події і допомагає швидко реагувати на інциденти. Інтелектуальні системи на основі штучного інтелекту та машинного навчання все частіше застосовуються для зменшення кількості хибних спрацьовувань і виявлення нових загроз у найкоротші строки.

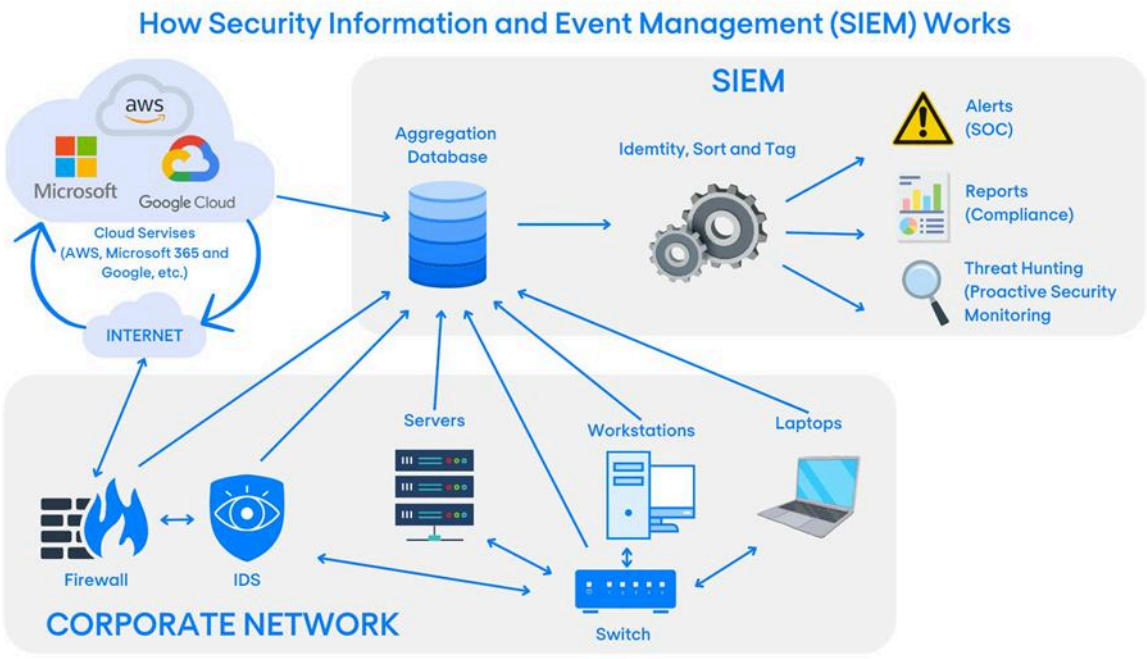

Рис. 2.3. Робота SIEM

Моніторинг та аналіз активності в хмарі здійснюється спеціалізованими системами, серед яких SIEM посідає центральне місце. Вона збирає дані з різних джерел, аналізує аномалії, автоматично оповіщає про підозрілі події і допомагає швидко реагувати на інциденти. Інтелектуальні системи на основі штучного інтелекту та машинного навчання все частіше застосовуються для зменшення кількості хибних спрацьовувань і виявлення нових загроз у найкоротші строки.

Важливий аспект - сегментація ресурсів і мереж, застосування обмежень, щоб користувачі або служби мали доступ тільки до безпосередньо необхідних даних - це принцип найменших привілеїв. Він мінімізує потенційні наслідки кіберінцидентів, якщо такі трапляються.

Впровадження політик резервного копіювання, їхнього шифрування і захисту створює додатковий бар'єр безпеки. Адже збереження копій даних у випадку технічних або кібератак дозволяє підтримувати безперервність бізнесу та швидко відновлювати операції.

Не менш важливою є відповідність нормативним вимогам - як загальним, так і галузевим. Провайдери хмарних послуг все більше піклуються про прозорість,

сертифікацію, аудити і гарантії безпеки, що стають аргументом для вибору їх у якості надійних партнерів.

Значну роль відіграють і питання людського фактора - навчання працівників, формування культури кібербезпеки, порядок дій у випадку інцидентів. Совісне ставлення до безпеки всередині організації разом із технічними заходами створюють міцний фундамент для довіри користувачів і успіху бізнесу.

Отже, безпека хмарних сервісів - це не тільки технології, а й стратегія, що поєднує інновації, стандарти і людський досвід, роблячи цифрове середовище надійним та зручним для використання.

2.6. Роль штучного інтелекту та машинного навчання в системах захисту

Автоматизація кібербезпеки сьогодні активно розвивається завдяки впровадженню технологій штучного інтелекту (ШІ) та машинного навчання. Традиційні методи захисту, засновані на сигнатурах та статичних правилах, часто не здатні ефективно протистояти сучасним атакам, які постійно змінюються та адаптуються. Стосовно цього, ШІ й МН дозволяють створювати динамічні системи, що автоматично виявляють аномалії, передбачають нові ризики і приймають оперативні рішення щодо захисту без людського втручання.

Основна ідея машинного навчання в галузі безпеки полягає у зборі та аналізі великих обсягів даних про мережеву активність, поведінку користувачів та події в системах. На основі цього формуються моделі норми, і коли відбуваються відхилення, вони виступають сигналом про потенційну загрозу. Різні типи алгоритмів (кластеризація, нейронні мережі, рекурентні моделі) застосовуються для розпізнавання складних патернів атак, що не можуть бути виявлені звичайними методами.

ШІ-технології інтегруються у сучасні системи виявлення вторгнень, SIEM та SOAR-платформи. Наприклад, системи SIEM на базі МН автоматично корелюють події з різних джерел, зменшуючи кількість помилкових спрацьовувань і

прискорюючи реакцію на інциденти. SOAR-рішення використовують штучний інтелект для автоматизації реакції: ізоляції загроз, зміни політик доступу і запуску розслідувань. Такий підхід дозволяє масштабувати безпекові операції, забезпечуючи різкі скорочення часу виявлення та нейтралізації атак.

Водночас важливо враховувати виклики: для ефективного навчання моделей потрібні якісні й актуальні дані, а також системи захисту від маніпуляцій і обману моделей зловмисниками. Незважаючи на це, автоматизація на основі ШІ змінює кібербезпеку, перетворюючи її з реактивної у більш проактивну та адаптивну систему захисту сучасних інформаційних середовищ.

2.7. Container та Kubernetes

Безпеку контейнерів можна уявити як захист великої кількості маленьких «коробок» з програмами, які запускаються на серверах. Ідея така: краще перевірити все ще до запуску, а потім мати багато шарів захисту під час роботи. Це називають підходами defense-in-depth (захист у глибину) та shift-left (перенесення перевірок безпеки на найранніший етап). Коли розробник створює контейнер, він пише Dockerfile - це як рецепт, де описано, що саме всередині коробки: яку операційну систему, яку версію програми, які додаткові бібліотеки потрібно. Існує також SBOM - це просто детальний список усіх «інгредієнтів» усередині контейнера. Спеціальні програми-сканери (наприклад, Trivy, Grype, Snyk) проглядають цей рецепт та список і шукають відомі «дірки» в безпеці, які вже мають свої офіційні номери (вони називаються CVE). CVSS - це шкала, яка показує, наскільки небезпечна дірка: чим більше число, тим гірше; наприклад, більше 7 означає, що проблема серйозна.

Ще одна важлива річ - фіксовані версії. Замість того, щоб писати «візьми останню доступну версію nginx», краще вказати конкретну - наприклад, nginx:1.25-alpine. Це називають «pinning versions». Так ви точно знаєте, що запускаєте перевірену збірку, а не раптово оновлену версію з новими багами. Multi-stage builds - це спосіб спочатку зібрати програму в «важкій» коробці з усіма інструментами, а потім перенести лише потрібні файли в дуже «легку» коробку. Такі мінімальні образи

називаються distroless або scratch - у них немає навіть командного рядка (shell) чи стандартних бібліотек, тому якщо зловмисник потрапить всередину, йому набагато важче щось зробити. Підпис provenance - це як поставити цифровий підпис під коробкою: хто її зібрав, коли і з чого. Цим займаються інструменти на кшталт cosign/Sigstore. Вони дозволяють перевірити, що образ справді з офіційного джерела, а не підмінений. Постквантові алгоритми (наприклад Kyber) - це просто нові схеми шифрування, які мають витримати атаки майбутніх квантових комп'ютерів. Склади для образів - це спеціальні сервери-реєстри, де ці коробки зберігаються (наприклад Harbor або Quay). Перед тим як Kubernetes дозволить запустити контейнер, у гру вступає «охоронець» - admission webhook: він перевіряє підпис, політики та вирішує, пускати чи ні.

Kubernetes, у свою чергу - це система, яка керує великою кількістю контейнерів на багатьох серверах. Щоб не було хаосу, у безпеці Kubernetes говорять про 4C: Cloud (хмара), Cluster (кластер K8s), Container (контейнери) та Code (код додатка). Pod - це найменша одиниця в Kubernetes, одна або кілька коробок, які завжди запускаються разом. Pod Security Admission - це набір правил, які кажуть, які pod'и дозволені. Наприклад, профіль Restricted забороняє pod'ам користуватися мережею та процесами хоста напряму (hostNetwork, hostPID, hostIPC) та не дозволяє «підвищувати» права всередині контейнера. Baseline — трохи м'який варіант, але теж не дозволяє запускати root-контейнери з привілеями. RBAC - це керування доступом на основі ролей: ServiceAccount - це технічний користувач для сервісу, а ClusterRole описує, що йому можна (наприклад тільки «читати список подів»). Це реалізує принцип «нульової довіри»: за замовчуванням нікому нічого не можна, кожен сервіс отримує мінімум прав.

Мережеві політики (NetworkPolicies) у Kubernetes керують тим, хто може з ким спілкуватися. За замовчуванням можна зробити «default deny», тобто заборонити весь трафік між pod'ами, а потім по трохи дозволяти потрібні зв'язки. Cilium або Calico - це спеціальні мережеві плагіни, що вміють фільтрувати трафік не тільки за IP та портами, а й за типом запитів на рівні застосунку. Вони використовують eBPF - це

технологія в Linux, яка дозволяє дуже швидко й гнучко втручатися в роботу мережі чи ядра системи.

Service Mesh, наприклад Istio, додає ще один рівень: між кожними двома сервісами ставиться маленький проксі (часто Envoy), і весь трафік між ними шифрується (mTLS - взаємне TLS, коли і клієнт, і сервер перевіряють один одного). Також можна налаштувати політики, які точно кажуть, які сервіси можуть викликати які, з якою швидкістю, з якими токенами (JWT) тощо. Це дозволяє виявляти й блокувати дивну поведінку.

Admission control - це загальна назва для всіх перевірок, які відбуваються перед тим, як Kubernetes прийме й запустить щось. Gatekeeper OPA чи Kyverno — це інструменти, які дозволяють записувати правила безпеки у вигляді коду: наприклад, «усі pod'и повинні мати певні мітки», «заборонити відкривати hostPort», «дозволяти образи лише з нашого офіційного реєстру». Secrets — це паролі, токени, ключі. Їх намагаються не зберігати у відкритому вигляді в Kubernetes, а брати на льоту з безпечних сховищ (Vault, AWS SSM) через спеціальних операторів або драйвери. SealedSecrets - це спосіб зберегти секрет у зашифрованому вигляді в Git, а розшифровка відбудеться тільки всередині кластера.

Runtime detection - це інструменти, які дивляться, що реально відбувається всередині контейнерів: Tetragon чи Falco відслідковують системні виклики й події на кшталт запуску оболонки (shell) у контейнері, спроби змінити системні файли або встановити пакети. Якщо таке трапляється, вони можуть відправити сповіщення в систему логів (ELK, Splunk) або навіть автоматично заблокувати под. Velero займається резервним копіюванням - робить знімки (snapshots) дисків і конфігурацій, часто в зашифрованому вигляді, щоб їх можна було відновити після аварії чи атаки. Журнали аудиту Kubernetes зберігають усі адміністративні дії: хто що створив, змінив або видалив, що важливо для розслідувань.

Нарешті, існують офіційні рекомендації та стандарти (CNCF, CIS), які говорять, як правильно налаштовувати Kubernetes: шифрувати внутрішню базу etcd, увімкнути правильні режими авторизації API-сервера, регулярно оновлювати сертифікати вузлів. Multi-tenancy означає, що кілька команд або проектів працюють у одному

кластері, але ізольовані через окремі простори імен (namespaces) та ліміти ресурсів. GitOps та інструменти типу ArgoCD дозволяють описати все це як код і автоматично застосовувати зміни з репозиторію, а моделювання загроз (наприклад, STRIDE) допомагає заздалегідь подумати, які саме атаки можливі на різні частини системи. Усе разом це перетворює Kubernetes з просто «оркестратора контейнерів» на платформу, де безпека закладена на кожному рівні - від коду й образів до мережі, прав доступу й моніторингу.

ВИСНОВКИ ДО РОЗДІЛУ 2

В цьому розділі узагальнено сучасні методи і засоби забезпечення кібербезпеки, зокрема криптографічні протоколи (TLS, IPsec, PGP, S/MIME) та системи виявлення й запобігання вторгненням (IDS/IPS) і SIEM. Показано, що комплексне застосування цих рішень та аналіз подій безпеки, що дає змогу суттєво знизити ризики успішних атак на інформаційно-комунікаційні системи.

РОЗДІЛ 3
АНАЛІЗ АКТУАЛЬНИХ КІБЕРЗАГРОЗ

3.1. Використання соціальної інженерії та фішингу

Соціальна інженерія - це один з найпотужніших інструментів злочинців у кіберпросторі, адже вона експлуатує найбільшу уразливість будь-якої системи - людський фактор. Замість того, щоб зламувати технічні захисти, зловмисники маніпулюють довірою, емоціями, необізнаністю чи поспіхом користувачів. Через такі психологічні трюки вони змушують людей добровільно розкривати паролі, відкривати шкідливі файли чи переходити за фальшивими посиланнями.

Особливу небезпеку становлять фішингові атаки, які часом виглядають настільки правдоподібно, що навіть обізнані користувачі можуть легко стати жертвами. Замість типових «масових розсилок» з підозрілими листами сьогодні атаки стають високоперсоналізованими - для цього зловмисники збирають дані з соцмереж, аналізують стиль спілкування, вподобання і навіть розклад жертви. Так з’явився AI-фішинг, який автоматично генерує тексти, що імітують реальне листування, збільшуючи шанси на успішний обман. У цьому ж руслі розвиваються дзвінки з синтезованим голосом (вішинг), де зловмисник видає себе за співробітника служби безпеки чи банку.

Атаки такого типу вже не виглядають як тривіальні шахрайства - це високоорганізовані психологічні операції, що ставлять за мету не просто крадіжку даних, а контроль над корпоративними системами, фінансовими активами чи репутацією. Соціальна інженерія охоплює фішинг, претекстинг, фізичний доступ, шахрайство через телекомунікації й навіть вплив за допомогою соціальних мереж і месенджерів.

Захист від соціальної інженерії вимагає багатогранного підходу. Технічні засоби, такі як антивірусні програми, системи фільтрації спаму, технології розпізнавання підроблених доменів, є необхідним базисом для попередження загроз.

Водночас саме постійне навчання і підвищення рівня кібергігієни серед співробітників є найбільш ефективним бар’єром, що знижує ризик успішної атаки. Організації впроваджують регулярні тренінги, тестування на стійкість до фішингу і системи імітаційних атак, що допомагає формувати культуру пильності.

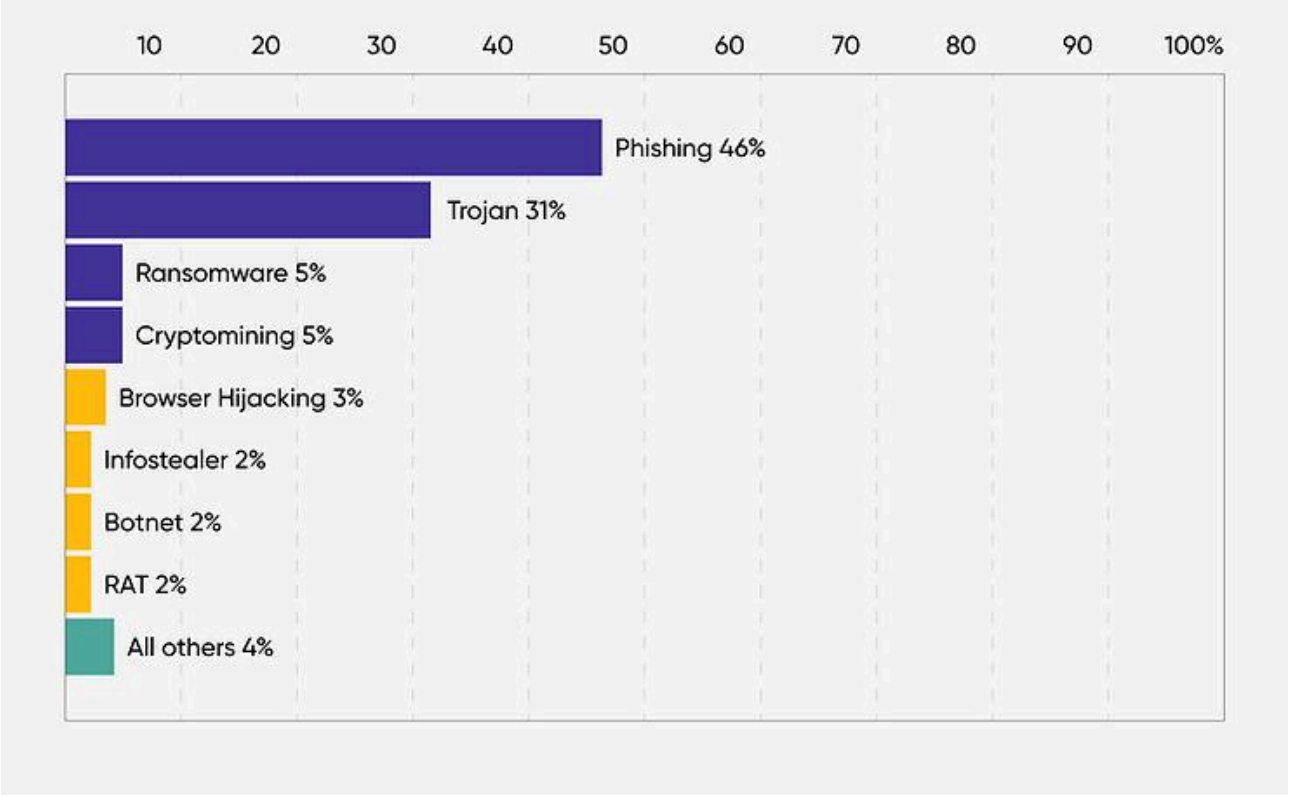

Рис. 3.1. Аналітика від Google

Серед усіх методів соціальної інженерії, фішинг залишається найпоширенішим інструментом кіберзлочинців. Його масштаб видно з численних аналітичних звітів: щодня в мережі циркулюють мільярди фішингових повідомлень, а великі технологічні компанії блокують значну їх частину ще до потрапляння до користувачів. За оцінками провідних постачальників кібербезпеки, суттєва частка всіх атак на організації припадає саме на фішинг, причому переважна більшість таких кампаній націлена на корпоративні електронні пошти та облікові записи. Це підтверджує, що фішинг залишається одним з найефективніших способів викрадення конфіденційних даних і проникнення в інформаційні системи.

Не менш значущим є моніторинг поведінки користувачів та аналіз їх активності, що дозволяє помітити аномалії й оперативно реагувати на потенційні загрози. Важливо поєднувати адекватні політики безпеки з відкритістю і підтримкою співробітників, щоб вони відчували відповідальність і розуміли загрози.

На законодавчому рівні збільшуються вимоги до захисту персональних і корпоративних даних, що стимулює бізнес впроваджувати ефективні механізми протидії фішингу і соціальній інженерії, захищаючи тим самим не лише власні активи, а й довіру клієнтів.

Фінальним елементом у боротьбі з цими загрозами є постійна адаптація та оновлення безпекових рішень, оскільки методи і технології зловмисників постійно вдосконалюються. Регулярне оновлення та комплексне застосування технологій і практик дозволяє стримувати атаки і підтримувати безпеку в цифровому середовищі.

Таким чином, соціальна інженерія та фішинг залишаються одними з найактуальніших і найнебезпечніших викликів кібербезпеки, що потребують комплексної стратегії захисту на основі технологій, навчання і контролю.

3.2. Вразливості дистанційних робіт

Перехід на дистанційну роботу відкрив широкі можливості для гнучкості бізнесу та ефективності співробітників, однак разом із цим це принесло серйозні виклики в сфері кібербезпеки. Основною проблемою стало те, що мережевий периметр розмився, а працівники почали підключатися до корпоративних ресурсів із різних нетипових або менш захищених середовищ, що створило нові вразливості.

Однією з найзначиміших уразливостей є недостатній рівень захисту домашніх і публічних мереж, якими користуються віддалені працівники. Часто їхні пристрої мають слабке, або застаріле програмне забезпечення, відсутній або неповний захист від шкідливого ПЗ. Вкладення поновлення операційних систем і антивірусів може бути непослідовним, що збільшує ймовірність компрометації.

Іншою проблемою є слабкий контроль доступу - у багатьох випадках немає достатніх механізмів багатофакторної автентифікації, що сильно полегшує

зловмисникам отримання доступу в разі викрадення облікових даних. Незахищений чи неправильно налаштований VPN-зв'язок часто стає точкою входу для атак, а відсутність централізованого моніторингу активності ускладнює виявлення аномалій і підозрілої поведінки в мережі.

Публічні Wi-Fi мережі, які використовують співробітники, будучи зручними, водночас піддають дані ризику перехоплення чи модифікації. Атаки типу «людина посередині» (MITM) можуть призвести до викрадення конфіденційної інформації навіть при наявності найкращих паролів.

Враховуючи ці проблеми, стратегія захисту від дистанційних вразливостей має базуватися на комплексі технічних, організаційних та освітніх заходів. По-перше, впровадження надійних VPN з сучасними алгоритмами шифрування та постійне оновлення їхніх компонентів дозволяє знизити ризики втручання у переданий трафік. Примусова багатофакторна автентифікація допомагає мінімізувати ймовірність несанкціонованого доступу, навіть якщо основний пароль був скомпрометований.

Ретельний контроль привілеїв користувачів відповідно до принципу найменших прав обмежує потенційні наслідки кіберінцидентів. Моніторинг, аналітика та кореляція даних про доступ і активність дають можливість вчасно виявляти незвичайну поведінку, наприклад одночасні спроби входу з різних геолокацій або незвичну активність у робочий час.

Ключовим елементом захисту є навчання співробітників - регулярні тренінги з кібергігієни, імітаційні атаки соціальної інженерії допомагають формувати у користувачів навички критичного мислення і правильних дій при підозрілих ситуаціях.

Також важливо впроваджувати політики безпеки, які регламентують використання робочих та особистих пристроїв, налаштування мережевих підключень і забезпечують контроль за використанням програмного забезпечення. Централізоване управління цими політиками і постійний аудит є критичними для масштабних компаній і організацій.

Загалом, враховуючи сучасні реалії, організації, які активно використовують дистанційні форми роботи, повинні адаптувати свої системи безпеки і підвищувати

культуру безпечної поведінки персоналу, щоб мінімізувати всі потенційні вразливості і забезпечити безперервність бізнес-процесів.

3.3. Проблеми безпеки MFA та PAM

Багатофакторна автентифікація (MFA) і управління привілейованим доступом (PAM) є надзвичайно важливими елементами комплексної стратегії кібербезпеки, спрямованими на захист найбільш чутливих систем та даних в організаціях різного рівня.

MFA значно ускладнює доступ зловмисникам завдяки додатковим рівням перевірки, що виходять за межі пароля - це можуть бути одноразові коди, біометрія чи push-повідомлення. Проте її впровадження пов’язане з певними викликами: складності в експлуатації для користувачів, необхідність наявності додаткових пристроїв, потенційні проблеми з відновленням доступу, а також появою нових методів обходу, як-от фішинг одноразових кодів і маніпуляції з push-повідомленнями. Крім того, не всі додатки та сервіси інтегрують MFA, що робить деякі зони вразливими.

Системи PAM відповідають за контроль і моніторинг користувачів із підвищеними правами доступу. Вони допомагають керувати привілейованими обліковими записами, обмежувати права, забезпечують аудит та виявлення аномальної поведінки. Застосування PAM допомагає мінімізувати ризики внутрішніх загроз і запобігти несанкціонованому доступу до критичних ресурсів. Однак їхнє впровадження може бути складним у великих або гетерогенних середовищах, а централізація контролю підвищує ризики у разі компрометації системи PAM.

Варто використовувати MFA і PAM, оскільки вони суттєво підвищують безпеку, знижують ризики компрометації внутрішніх та зовнішніх загроз, дозволяють забезпечити відповідність нормативним вимогам і підтримують високий рівень довіри партнерів і клієнтів. Разом вони утворюють багаторівневий захист, який важко обійти, значно зменшуючи потенційну площу атаки.

Для успішного впровадження MFA і PAM рекомендовано забезпечувати зручність користувачів, вести постійне навчання і підвищення обізнаності персоналу, строго дотримуватися внутрішніх політик безпеки, інтегрувати рішення у загальну безпекову архітектуру компанії, автоматизувати моніторинг і аудит дій.

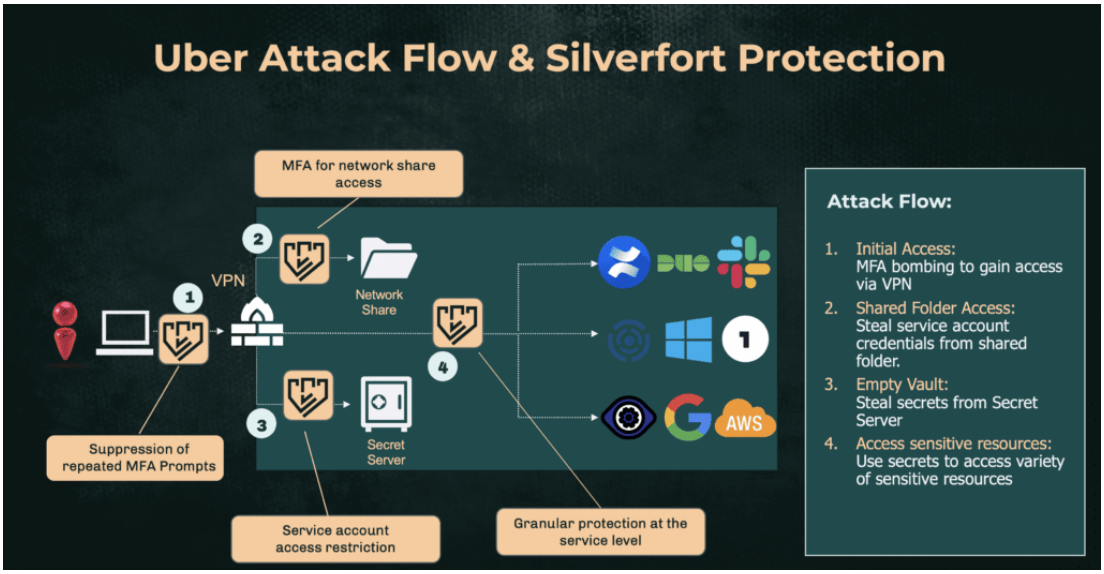

Рис. 3.2. Ілюстрація MFA і PAM

Оволодіння цими механізмами дозволяє організаціям ефективно захищати свої критично важливі ресурси від сучасних кіберзагроз, мінімізувати людські помилки та підвищувати стійкість інформаційних систем до злочинних дій.

3.4. Типові атаки на мережі та веб-додатки

Атаки на мережі та веб-додатки є одними з найстійкіших та найпоширеніших кіберзагроз, що завдають суттєвих збитків організаціям різного масштабу. Вони використовують вразливості мережевих протоколів, програмного забезпечення та помилки в конфігурації, а також маніпулюють поведінкою користувачів, що робить їх надзвичайно небезпечними.

Одним із найчастіших видів атак є DDoS-атаки (Distributed Denial of Service). Зловмисники використовують мережі заражених пристроїв - ботнети, щоб спрямувати величезний обсяг трафіку на цільові сервери чи мережеві пристрої, тим

самим викликаючи їхнє перевантаження і відмову в обслуговуванні. Такі атаки можуть тривати години або навіть дні, завдаючи шкоду бізнесу через недоступність сервісів і втрату клієнтів.

Атаки на мережеві протоколи, зокрема ARP spoofing та IP spoofing, дозволяють зловмисникам підмінити чи перехопити трафік, змінити дані або впровадити власні команди. DNS-спуфінг вводить користувачів у оману, перенаправляючи їх на шкідливі сайти замість легітимних. Такі атаки часто слугують початковою стадією для більш складних вторгнень.

Веб-додатки особливо вразливі до SQL-ін’єкцій, де через необроблені запити до бази даних зловмисник отримує можливість викрадати або змінювати конфіденційну інформацію. Cross-Site Scripting (XSS) відкриває шлях для впровадження шкідливих скриптів, які можуть викрадати сесійні дані користувачів, змінювати контент сторінок або запускати атаки на інші сайти від імені заволоділи користувачів.

Проблеми аутентифікації і управління сесіями часто використовуються для обходу захисту. Brute force-атаки шляхом послідовного підбору паролів дозволяють зловмисникам отримати доступ до облікових записів. Використання вкрадених токенів дає змогу заводити сесії без повторної автентифікації.

API, які стають серцем сучасних складних систем, складають особливий клас уразливостей. Неправильна настройка, слабкі механізми автентифікації та відсутність контролю обмежує потенціал цих точок атак, що можуть призводити до витоку даних або повного контролю над системою.

Захист від загроз вимагає комплексного підходу: використання сучасних технічних засобів - веб-фаєрволів, систем виявлення вторгнень, регулярних оновлень програмного забезпечення, обмеження прав користувачів, аудитів безпеки. Особливо важливе проведення навчань для користувачів і розробка ефективних механізмів реагування на інциденти.

Ефективна безпека в мережах і веб-додатках - це результат постійної боротьби між захисниками та атакувальниками, де проактивність, швидкість реагування і глибина аналізу можуть стати вирішальними факторами.

3.5. Моніторинг і аудит мережевої безпеки

Моніторинг і аудит є ключовими процесами забезпечення безпеки інформаційних систем, що дозволяють у реальному часі контролювати події в мережі та оцінювати ефективність заходів захисту. Моніторинг означає збір і аналіз логів і сигналів з усіх комунікаційних пристроїв і систем, а аудит включає систематичний огляд політик, конфігурацій, вразливостей і відповідності нормативним вимогам.

Основним інструментом моніторингу є SIEM-системи, що централізують інформацію про безпеку від фаєрволів, серверів, комутаторів, систем автентифікації та захисту, виконують кореляцію подій і аналіз аномалій. Сучасні SIEM платформи застосовують машинне навчання для зниження рівня хибних тривог і вдосконалення пріоритезації загроз.

Для контролю мережевого трафіку використовують Network Traffic Analyzers і Network Packet Brokers, які допомагають виявляти приховані або аномальні канали зв’язку, навіть якщо трафік шифрований. Аналіз трафіку з використанням ШІ підвищує здатність знаходити складні й багатоступеневі атаки.

Аудит безпеки передбачає регулярне сканування вразливостей, тестування на проникнення, перевірку конфігурацій пристроїв і відповідність стандартам, таким як ISO 27001, GDPR, PCI DSS. Для цього застосовують спеціалізовані платформи управління вразливостями, які автоматизують процес виявлення, пріоритезації, усунення і перевірки.

Найкращі практики передбачають багаторівневий моніторинг із цілодобовим контролем критично важливих систем, автоматизованою кореляцією подій, використанням аналітичних панелей та чітким розподілом обов’язків між аналітиками різних рівнів. Інтеграція таких систем із SOAR-платформами значно підвищує ефективність реакції на інциденти і загальну безпеку корпоративної мережі.

ВИСНОВКИ ДО РОЗДІЛУ 3

В цьому розділі проаналізовано нормативно-правову базу та міжнародні стандарти, зокрема ISO/IEC 27001, NIST Cybersecurity Framework і GDPR, а також сучасні практики аутентифікації, керування доступом, MFA та PAM. Доведено, що орієнтація на ці стандарти й регламенти дозволяє системно підходити до управління ризиками, формування політик безпеки та побудови зрілої системи менеджменту інформаційної безпеки.

РОЗДІЛ 4
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КОРПОРАТИВНОЇ ІКС

Сучасні підприємства у сфері інформаційних технологій потребують надійної, масштабованої та безпечної мережевої інфраструктури для забезпечення ефективної роботи всіх підрозділів. Компанія ASAP DM, яка спеціалізується на розробці, впровадженні та супроводі інформаційних систем для бізнесу, не є винятком.

Метою даного дослідження є аналіз існуючої мережевої інфраструктури підприємства ASAP DM та розробка рекомендацій щодо її оптимізації з урахуванням специфіки діяльності компанії, вимог безпеки різних відділів та необхідності забезпечення стабільної роботи критично важливих сервісів.

Актуальність дослідження обумовлена зростаючими потребами підприємства у надійних мережевих рішеннях, необхідністю забезпечення високого рівня інформаційної безпеки та оптимізації витрат на підтримку IT-інфраструктури.

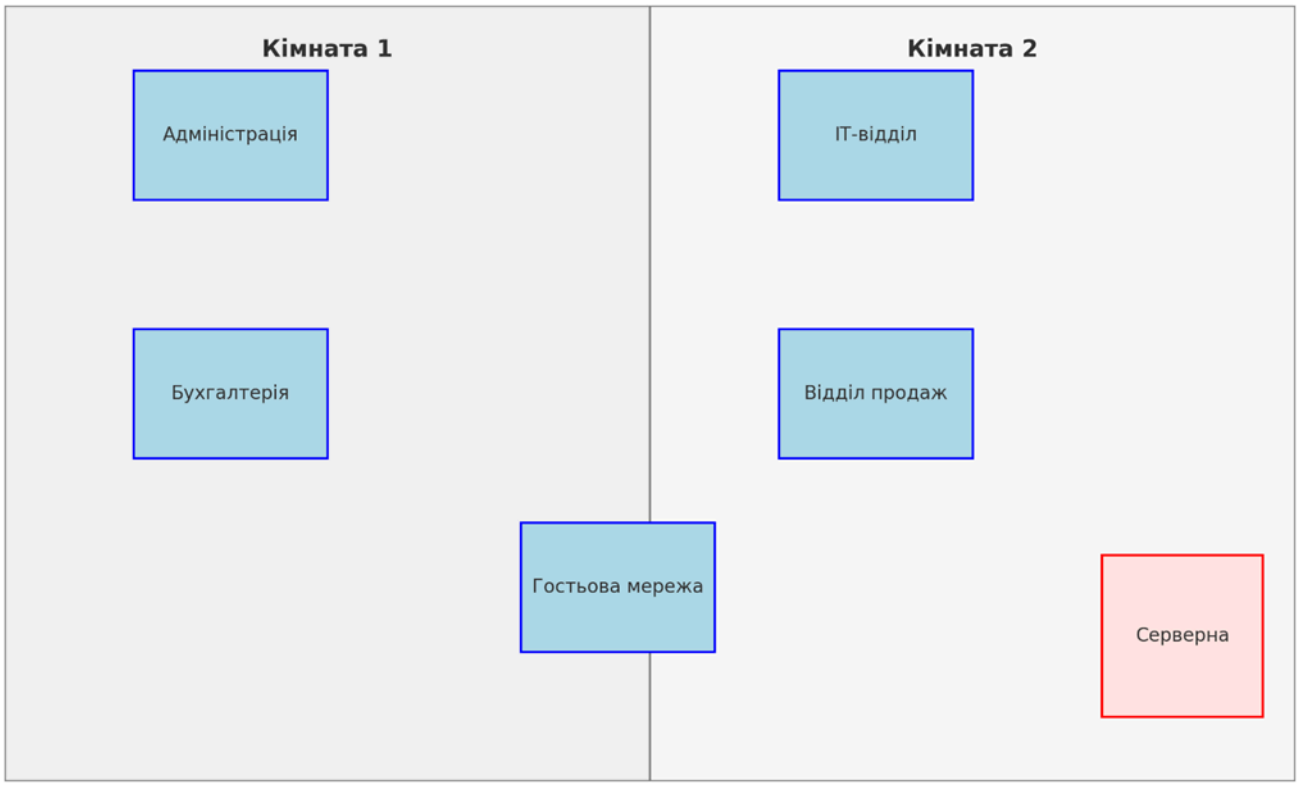

Рис. 4.1. План приміщення одноповерхового офісу

4.1. Створення логічної топології локальної мережі в середовищі Cisco Packet Tracer

На першому етапі проєктування було здійснено розміщення логічних компонентів мережі підприємства "ASAP DM" у віртуальному середовищі моделювання Cisco Packet Tracer. Побудова топології дозволяє наочно представити фізичну структуру майбутньої мережі, визначити типи обладнання, взаємозв’язки між ними та забезпечити умови для подальшої конфігурації пристроїв.

Перелік мережевого обладнання:

Маршрутизатор (1 шт) - для реалізації маршрутизації; Керовані комутатори - для обслуговування кінцевих пристроїв та підтримки VLAN; Сервери - реалізує служби DHCP, DNS та VPN-сервіси; Кінцеві пристрої - розподілені між п’ятьма відділами підприємства.

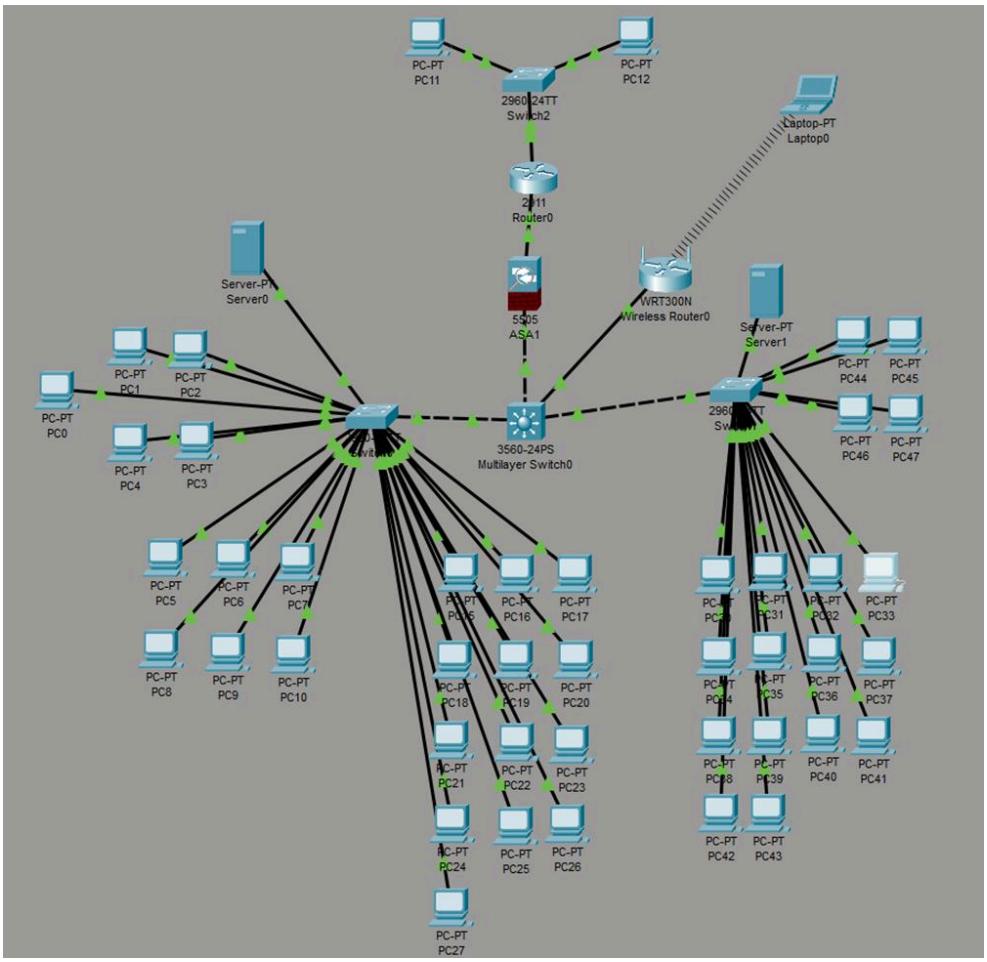

Рис. 4.2. Схема підключення

Структура мережі: Топологія побудована на основі класичної ієрархічної моделі з використанням дворівневої структури доступу. Кожен комутатор під’єднаний до маршрутизатора через транковий порт для забезпечення передачі VLAN-трафіку, що дає змогу реалізувати сегментацію мережі за допомогою віртуальних локальних мереж.

Комутатор SW1 обслуговує відділи: Адміністрація (VLAN 10); Бухгалтерія (VLAN 20); IT-відділ (VLAN 30).

Комутатор SW2 обслуговує: Відділ продаж (VLAN 40); Гостьова мережа (VLAN 50);

Кожна VLAN має власний IP-діапазон у межах підмережі 192.168.10.0/24 з маскою 255.255.255.0, що дозволяє логічно ізолювати трафік різних підрозділів підприємства.

4.2. Налаштування маршрутизатора для міжвіртуальної маршрутизації

Одним із ключових етапів побудови корпоративної мережі є логічна сегментація, яка досягається шляхом використання віртуальних локальних мереж (VLAN). Такий підхід дозволяє ефективно розділити трафік між відділами підприємства, підвищити рівень безпеки, зменшити кількість широкомовного трафіку та спростити адміністрування.

Налаштування VLAN на комутаторах: Комутатор SW1 (обслуговує VLAN 10, 20, 30).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name ADMIN
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name ACCOUNTING
Switch(config-vlan)#vlan 30 IT
                    ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#vlan 30
Switch(config-vlan)#name IT
VLAN #50 and #30 have an identical name: IT
Switch(config-vlan)#vlan 50
Switch(config-vlan)#name GUEST
Switch(config-vlan)#configure terminal
                    ^
% Invalid input detected at '^' marker.
```

Рис. 4.3. Створення VLAN

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1 - 5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface range fa0/6-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#interface range fa0/6-11
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#interface range fa0/12-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#
```

Рис. 4.4. Призначення портів, налаштування транкового порту

Комутатор SW2 (обслуговує VLAN 40, 50)

Створення VLAN та призначення портів, налаштування транкового порту:

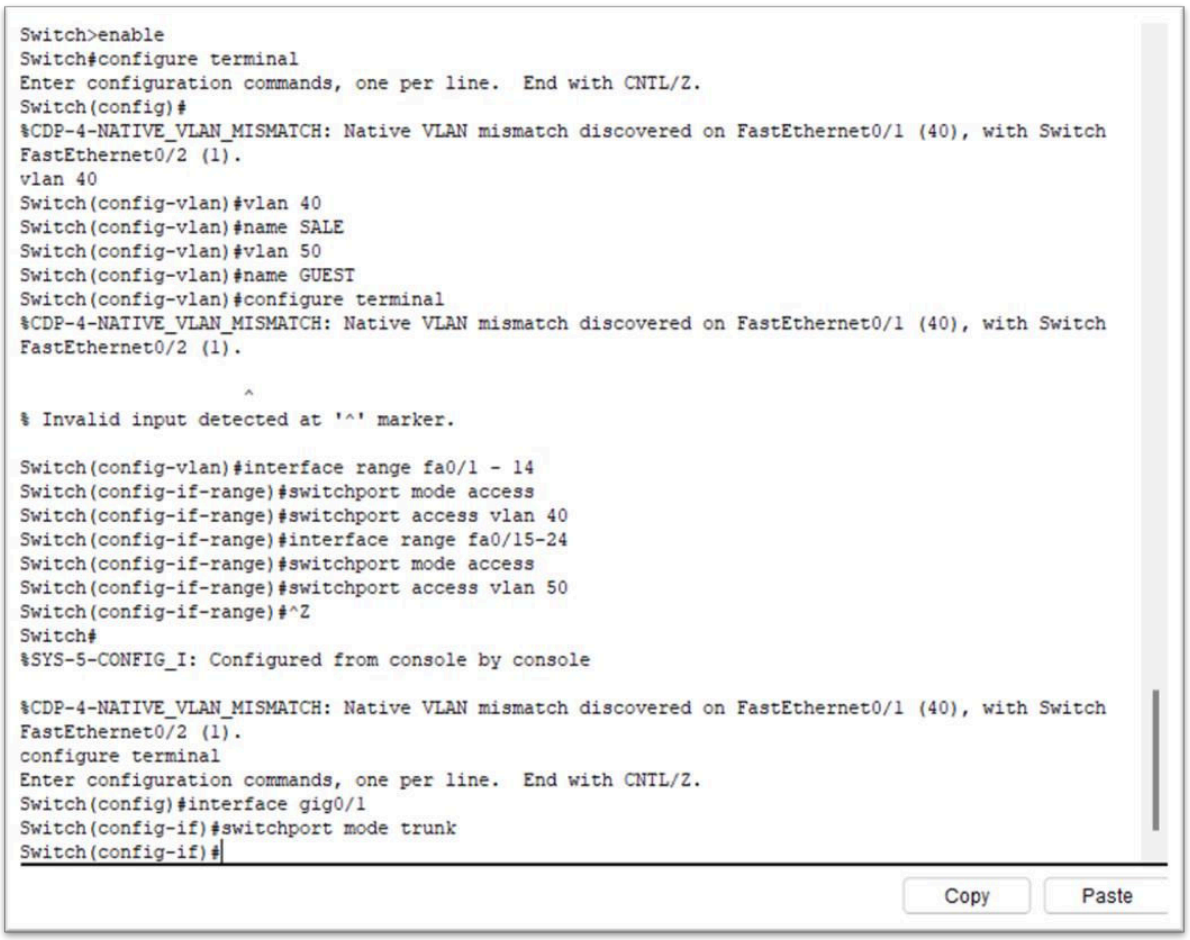

Рис. 4.5. Створення VLAN та призначення, налаштування транкового порту

4.3. Налаштування DHCP на сервері та створення DHCP-пулів на сервері

Потрібно забезпечити автоматичну видачу IP-адрес для пристроїв у кожній VLAN за допомогою централізованого DHCP-сервера, розміщеного в локальній мережі.

DHCP-сервер — фізичний або віртуальний сервер у VLAN 10 (ADMIN), під'єднаний до Switch0.

DHCP обслуговує всі VLAN: 10, 20, 30, 40, 50.

DHCP-сервер бачить усі VLAN завдяки маршрутизації на WS-C3560 (ip routing).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gig0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#
```

Рис. 4.6. DHCP-сервер

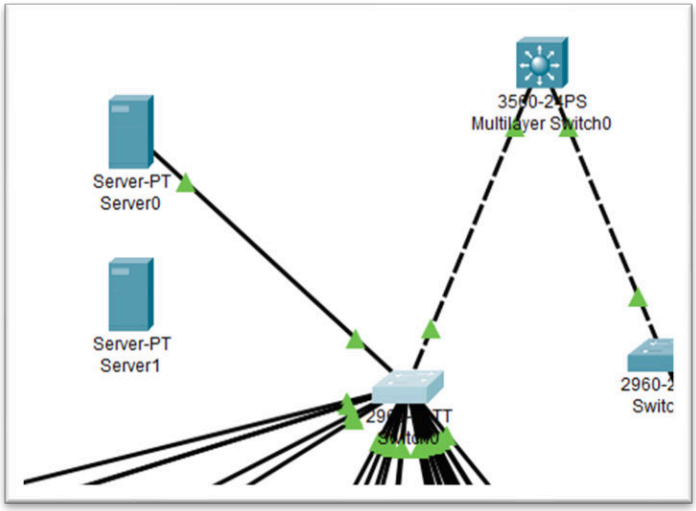

Рис. 4.7. Підключаємо сервер до access-порту VLAN 10 на Switch0

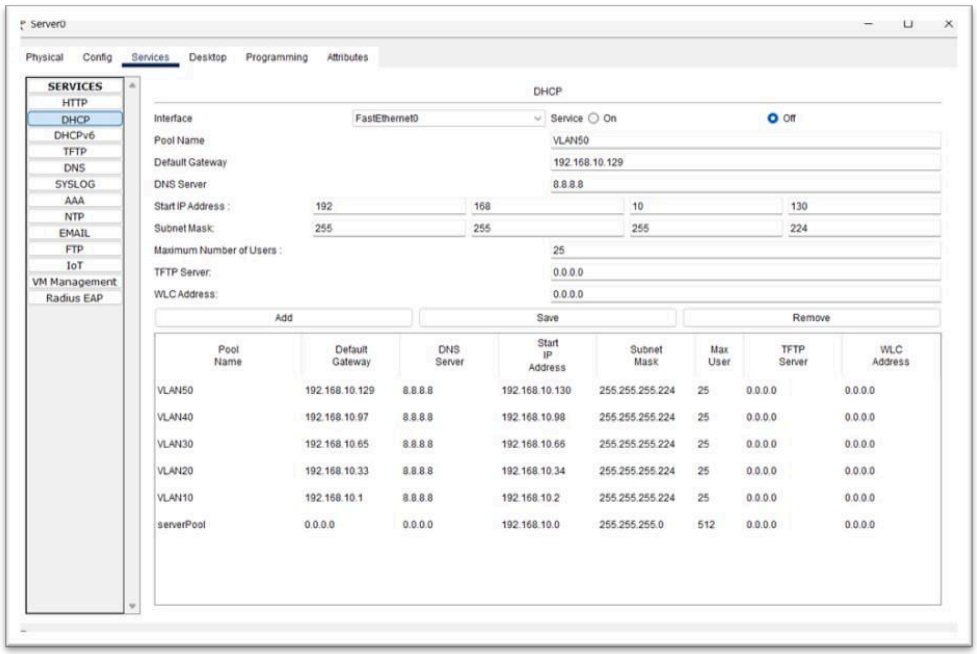

Рис. 4.8. Створення DHCP-пулів на сервері

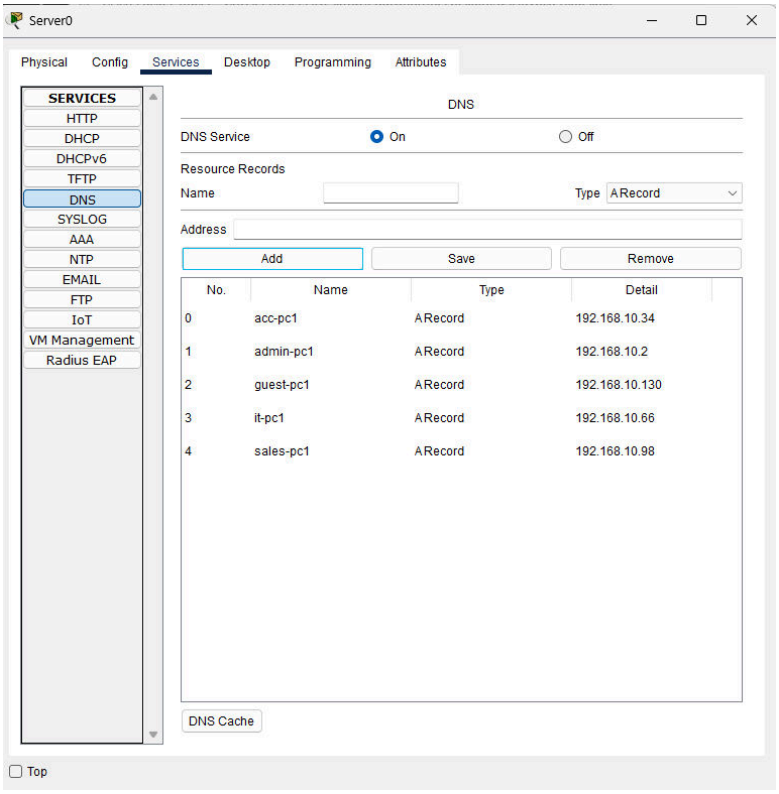

Рис. 4.9. Налаштування DNS-сервісу

4.4. Налаштування

```
Switch(config)#interface vlan 50
Switch(config-if)# ip access-group 50 in
Switch(config-if)#
```

Рис. 4.10. Ізоляція гостьової VLAN 50 від решти

```
Switch(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (99), with Switch
FastEthernet0/1 (40).
ip access-list extended BLOCK-SALES
Switch(config-ext-nacl)#permit ip 192.168.10.96 0.0.0.31 host 192.168.10.10
Switch(config-ext-nacl)#deny ip 192.168.10.96 0.0.0.31 192.168.10.0 0.0.0.255
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (99), with Switch
FastEthernet0/1 (40).

Switch(config-ext-nacl)#permit ip any any
Switch(config-ext-nacl)#exit
Switch(config)#
```

Рис. 4.11. Дозволити лише частковий доступ VLAN 40 (Продажі)

Політика безпеки:

Блокуємо будь-який трафік з VLAN 50 (гостьова мережа) до внутрішніх адрес, VLAN 40 (відділ продажів) має доступ лише до двох серверів: 192.168.10.10 (DHCP/FTP) та 192.168.10.11 (DNS).

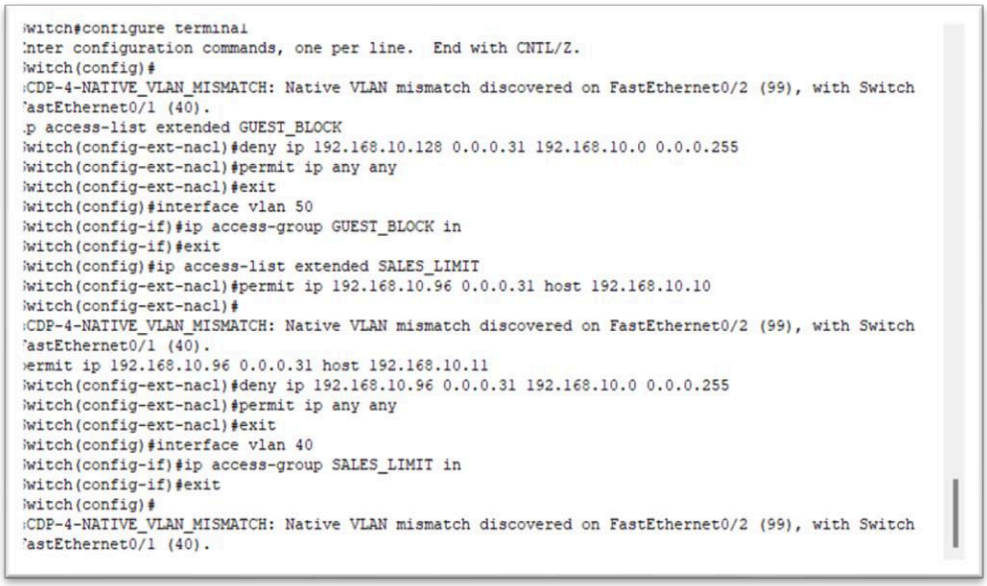

Рис. 4.12. Блокуємо будь-який трафік з VLAN 50 (гостьова мережа)

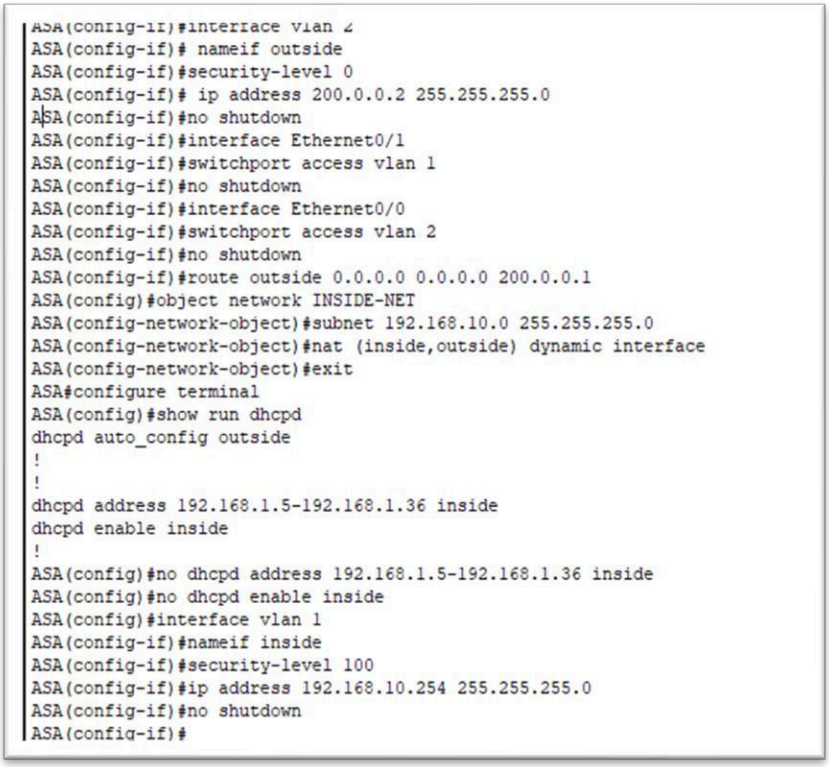

Рис. 4.13. Блокуємо будь-який трафік з VLAN 50

```
Switch(config-if)#interface FastEthernet0/5
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
% 192.168.10.0 overlaps with Vlan10
Switch(config-if)#ip address 192.168.11
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/2 (99), with Switch
FastEthernet0/1 (40).
.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#description Link to ASA
Switch(config-if)#
```

Рис. 4.14. Налаштування Екрану Cisco ASA для Роутеру 3560 для Cisco ASA

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)# ip address 200.0.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)#
```

Рис. 4.15. Налаштування Роутеру 2911 для Cisco ASA

4.5. Підключення точки доступу Wi-Fi до корпоративної мережі

Згідно із сучасними вимогами до корпоративної мережевої інфраструктури, для забезпечення належної ізоляції мережевого трафіку та підтримки кількох підмереж (VLAN) впроваджується trunk-з'єднання між комутатором і точкою доступу Wi-Fi (WRT300N)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface gigabitEthernet0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40,50
Switch(config-if)#switchport trunk native vlan 40
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#
```

Рис. 4.16. Впровадження WI-FI

На комутаторі конфігурується фізичний порт, активується режим trunk (switchport mode trunk) для підтримки передачі пакетів різних VLAN.

Дозволяється проходження трафіку усіх необхідних VLAN (switchport trunk allowed vlan 10,20,30,40,50).

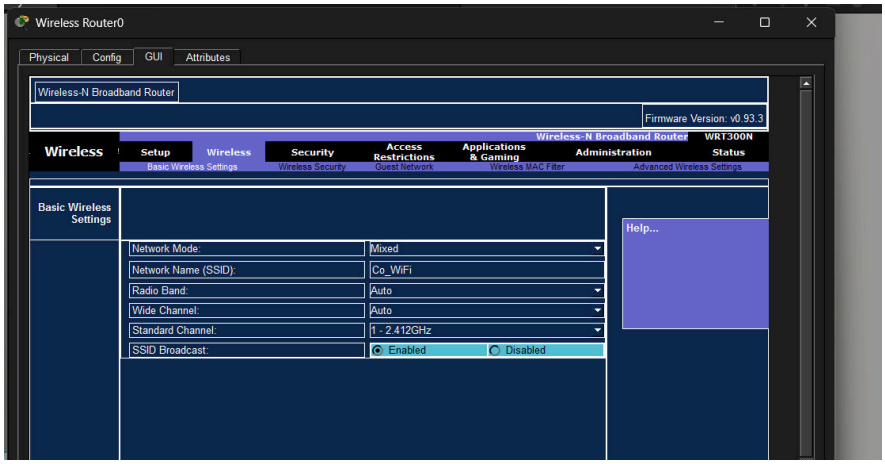

Рис. 4.17. Налаштування

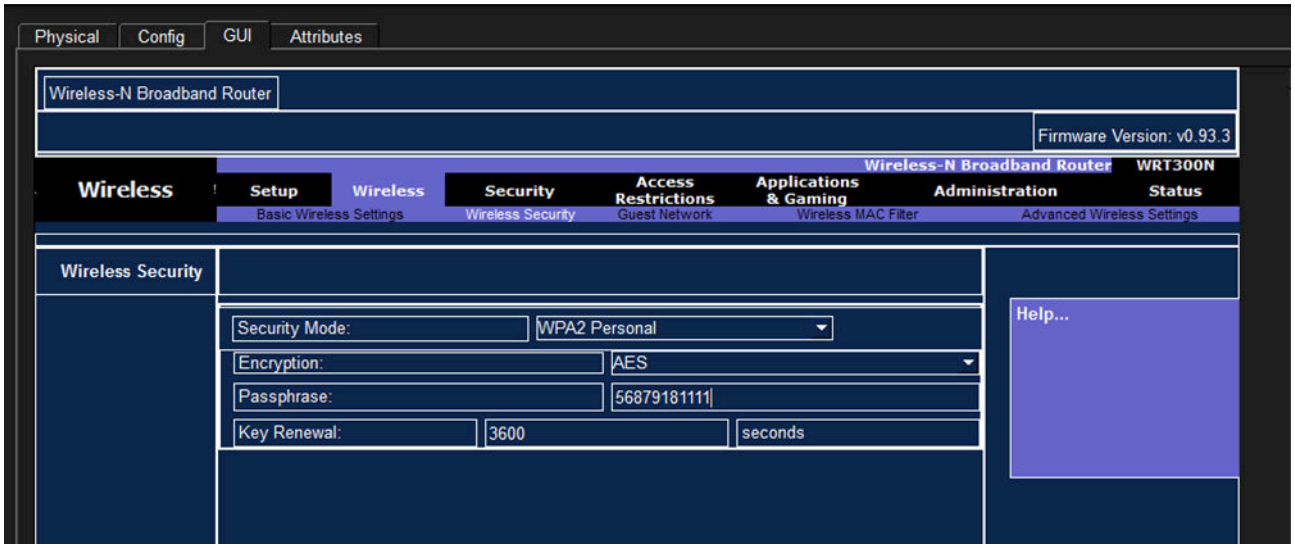

Рис. 4.18. Налаштування

Після реалізації пристрою trunk-з’єднання та створення захисту, можливе підключення клієнтського пристрою - ноутбука до відповідного SSID точки доступу Wi-Fi. Кожен SSID відповідає певній VLAN та має власну політику доступу й налаштування безпеки.

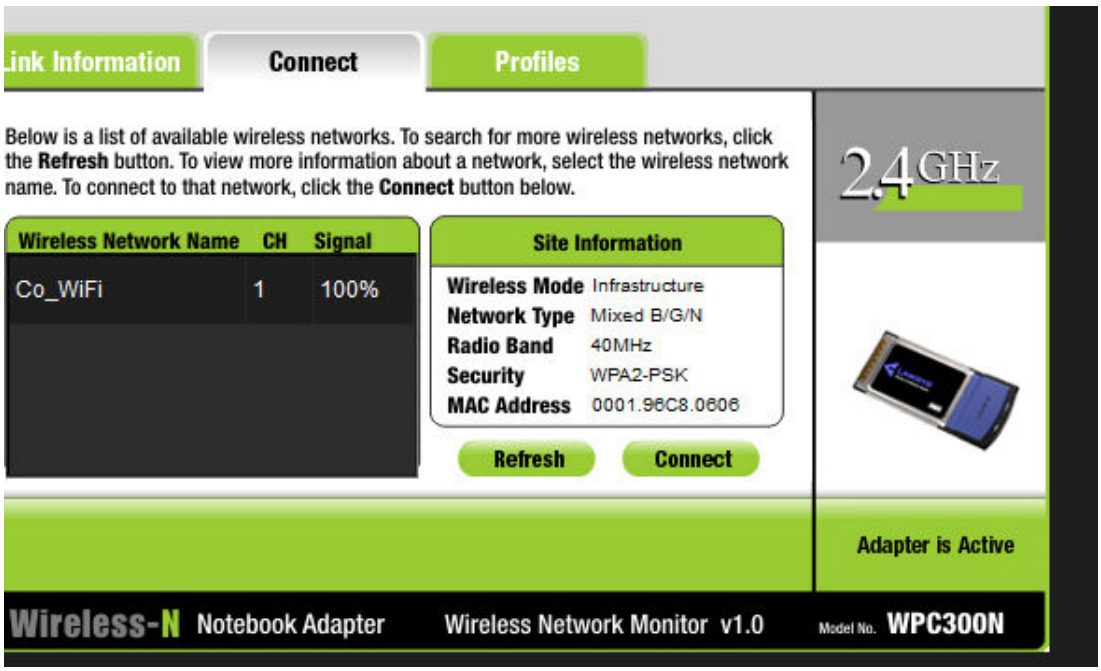

Рис. 4.19. Налаштування

Рис. 4.20. Налаштування

Підключившись до мережі, ноутбук автоматично отримує IP-адресу через механізм DHCP, відповідно до VLAN, до якої прив'язано обране SSID. Подальше функціонування ноутбука здійснюється у межах відповідної підмережі - користувач отримує доступ тільки до визначених ресурсів, що відповідає принципам корпоративної безпеки. Забезпечується мережна ізоляція і контрольований доступ до службових або гостьових сервісів підприємства.

4.6. Логічна структура мережі

IP-планування (IPv4):

У локальній мережі підприємства використовується приватна адресація IPv4 на основі діапазону 192.168.10.0/24. Кожен відділ розміщено в окремій VLAN, для якої виділена окрема підмережа з маскою /27 (тобто до 30 хостів на VLAN).

Таблиця 4.1

Таблиця IP-адресування по VLAN

VLAN	Назва відділу	IP-адресація	Gateway	DHCP діапазон
10	ADMIN	192.168.10.0/27	192.168.10.1	192.168.10.2 – .30
20	ACCOUNTING	192.168.10.32/27	192.168.10.33	192.168.10.34 – .62
30	IT	192.168.10.64/27	192.168.10.65	192.168.10.66 – .94
40	SALES	192.168.10.96/27	192.168.10.97	192.168.10.98 – .126
50	GUEST	192.168.10.128/27	192.168.10.129	192.168.10.130 – .158
	Сервери	VLAN 10	—	Статична адресація

DHCP-сервер розміщено в VLAN 10 (адреса 192.168.10.10). Він обслуговує всі VLAN, завдяки маршрутизації на WS-C3560. Кожна VLAN має окремий DHCP-пул. DNS та шлюз призначаються автоматично через DHCP.

DNS-сервер також у VLAN 10, IP 192.168.10.11. Відповідає за розпізнавання доменних імен у внутрішній мережі. Вручну додані записи типу: admin-pc1 → 192.168.10.2, а також ftp-server → 192.168.10.10.

4.7. Приклади атак

У Cisco Packet Tracer можна практично відтворити типові мережеві атаки. Це дасть змогу побачити, як зловмисники можуть використовувати слабкі місця в мережі, і водночас зрозуміти, як працюють базові засоби захисту.

Ping Flood (ICMP DoS)

Атака починається з ПК33 на Сервер2.

Зловмисник виконує дуже багато разів команду надсилання ICMP Echo Request до IP-адреси цільового сервера «ping 192.168.40.10».

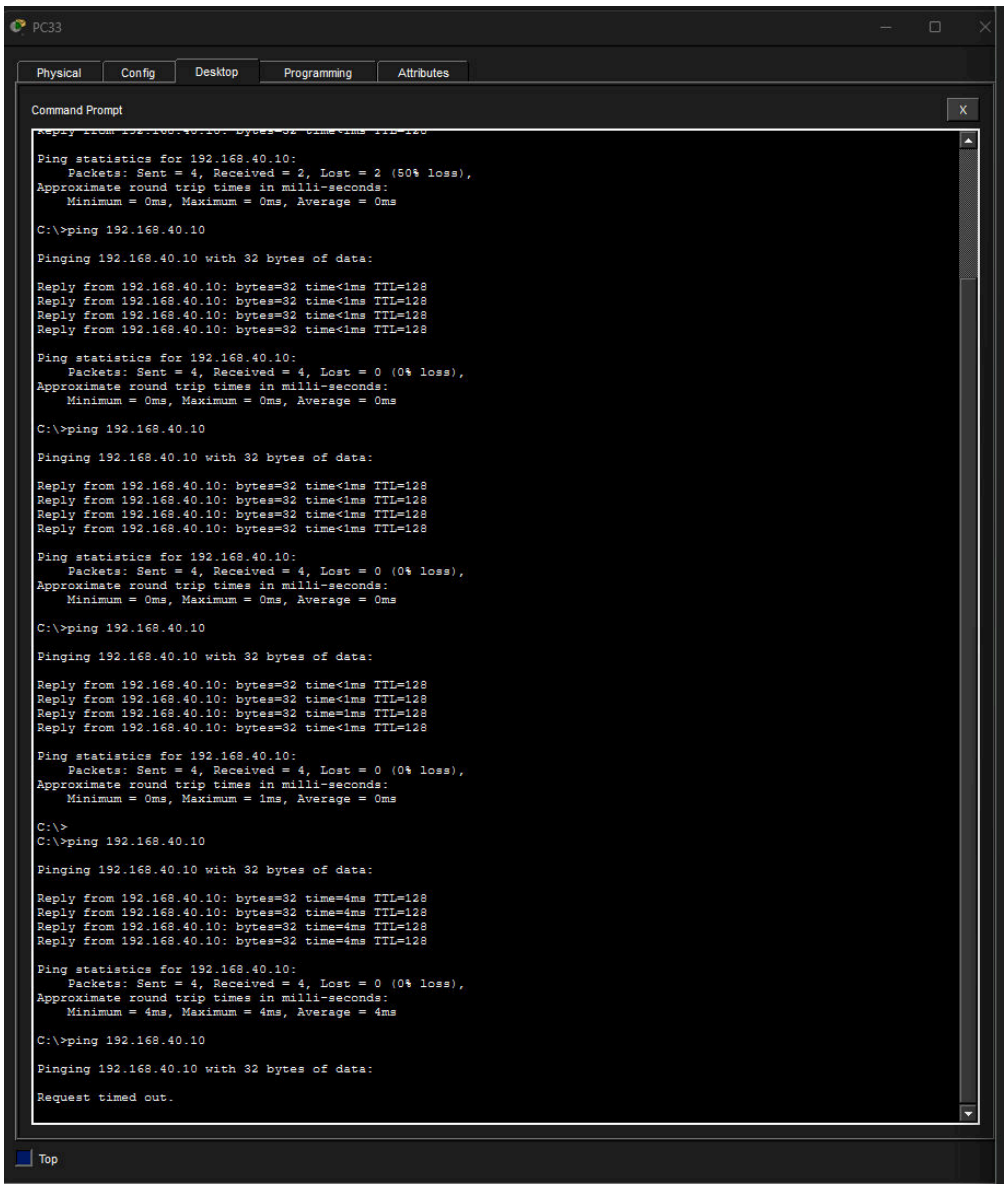

Рис. 4.21. Демонстрація

І в кінцевому результаті ми бачимо що сервер перестав відповідати на запити через перевантаження.

Ping Flood показує, що неконтрольований ICMP-трафік може легко перевантажити навіть простий сервер, зробивши мережу непрацездатною для звичайних користувачів. Це гарна демонстрація для дослідження впливу DoS-атак і потреби мережевих захистів.

Для захисту від Ping Flood-атаки слід комплексно застосовувати обмеження швидкості ICMP-трафіку (rate limiting), списки контролю доступу ACL для блокування масових ping-запитів, фільтрування ICMP на маршрутизаторах і використання брандмауерів для детекції та блокування flood-потоку.

VLAN Hopping

VLAN Hopping — атака, при якій пристрій з однієї VLAN отримує несанкціонований доступ до трафіку іншої VLAN. Зазвичай здійснюється через експлуатацію режиму trunk або Dynamic Trunking Protocol (DTP).

Атакуючий - ПК46 у VLAN 50 (гостьова), FastEthernet0/16, а жертва - ПК33 у VLAN 40 (корпоративна), FastEthernet0/5.

Зловмисник на комутаторі змінює режим порту FastEthernet0/16 (де знаходиться ПК44) із access на trunk.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet0/16
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to up
switchport trunk allowed vlan all
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#
```

Рис. 4.22. Зміна режиму порту

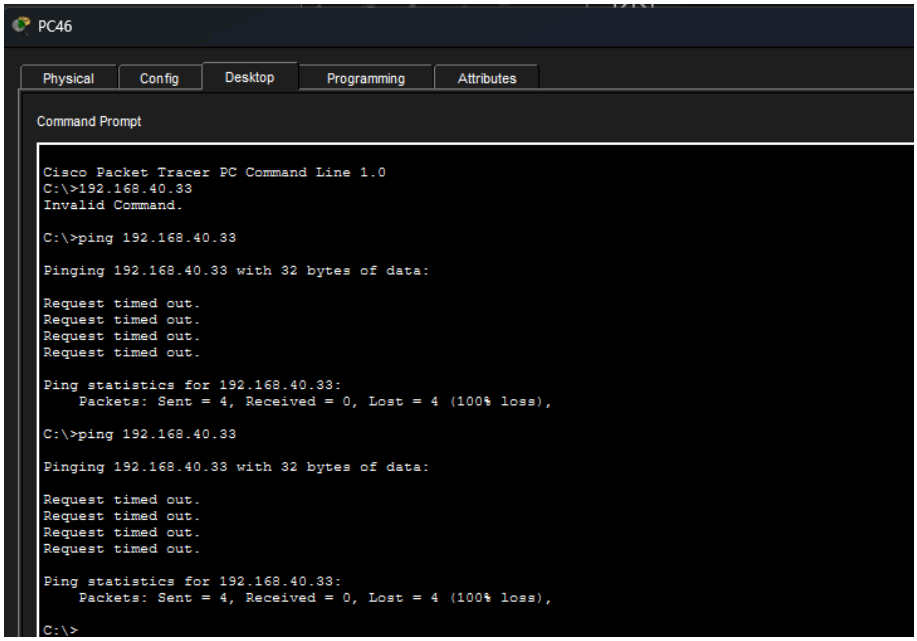

Рис. 4.23. Демонстрація

На скріншоті продемонстровано що ізоляція гостьової VLAN працює коректно та цей спосіб не вдалось реалізувати зловмиснику. VLAN Hopping показує критичну важливість правильної конфігурації портів комутатора. Помилка в налаштуванні режиму портів дозволяє навіть гостьовим пристроям отримувати несанкціонований доступ до захищених мереж.

Демонстрація проведена у Packet Tracer через зміну типу порту гостьового ПК із access на trunk, що імітує помилки або маніпуляції в налаштуваннях комутатора. Це найпоширеніший сценарій VLAN Hopping який дозволяє показати ризики некоректної конфігурації гостьових та користувацьких портів.

ВИСНОВКИ ДО РОЗДІЛУ 4

В практичному розділі продемонстровано модель корпоративної мережі в Cisco Packet Tracer із налаштуванням маршрутизації, DHCP, DNS, VLAN-сегментації та

захисту Wi-Fi, проведено тестування атак та заходів протидії показало ефективність запропонованих механізмів захисту й підтвердило працездатність розробленої архітектури з позицій кібербезпеки.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

У процесі розробки та експлуатації інформаційно-комунікаційних систем (ІКС) корпоративної мережі важливо враховувати не лише технічну ефективність та безпеку, але й екологічний вплив такої діяльності. Професійна діяльність інженера з кібербезпеки пов’язана з використанням значної кількості мережевого та серверного обладнання, систем живлення й кондиціонування, що прямо впливають на споживання електроенергії, утворення відходів електронного та електротехнічного обладнання, а також на мікроклімат приміщень. Актуальність екологічного аспекту зумовлена глобальними тенденціями до зниження вуглецевого сліду IT-інфраструктур, впровадженням «зеленої» енергетики та вимогами екологічного законодавства до поводження з відходами електроніки.

У межах тематики дипломної роботи основними джерелами впливу на навколишнє середовище є:

- Споживання електроенергії серверним та мережевим обладнанням (маршрутизатори, комутатори, точки доступу, сервери, системи збереження даних), що опосередковано призводить до викидів парникових газів при її генерації.
- Системи кондиціонування та вентиляції серверних приміщень, які забезпечують відведення тепла від обладнання, але при цьому підвищують загальне енергоспоживання та потребують використання холодоагентів.
- Утворення відходів електронного та електротехнічного обладнання (вийшли з ладу або морально застарілі комутатори, маршрутизатори, блоки живлення, кабельні системи, акумулятори UPS).
- Використання витратних матеріалів (пластикові конектори, ізоляційні матеріали, упаковка від обладнання), що при неналежній утилізації потрапляють на полігони твердих побутових відходів.

Ці впливи належать переважно до фізичного (енергоспоживання, тепловиділення) та хімічного (наявність важких металів і токсичних компонентів в електроніці) факторів, а також до сфери поводження з відходами, що є характерним для сучасних дата-центрів та корпоративних мережевих інфраструктур.

5.1. Фактори

Найбільш вагомим фактором у контексті даної роботи є підвищене енергоспоживання мережевої інфраструктури та пов'язані з ним побічні ефекти. Тривала робота серверів, комутаторів і обладнання без режимів енергозбереження призводить до значних витрат електроенергії, що у масштабі підприємства формує відчутний вуглецевий слід. Це супроводжується виділенням значної кількості тепла, яке необхідно відводити системами кондиціонування, що ще більше збільшує загальне енергоспоживання. У результаті зростає навантаження на енергосистему, збільшуються викиди CO_2 та інших шкідливих речовин на станціях генерації електроенергії.

Другим суттєвим впливом є накопичення відходів електронного обладнання. Комутатори, маршрутизатори, материнські плати, блоки живлення містять важкі метали (свинець, ртуть, кадмій), бромовані антипірени та інші небезпечні компоненти. При неконтрольованому захороненні чи спалюванні такі відходи призводять до забруднення ґрунтів і вод, потрапляння токсичних речовин у харчові ланцюги та негативного впливу на здоров'я людей. Неправильне поводження з акумуляторами (UPS, резервні батареї) спричиняє ризики витоку електролітів та важких металів у навколишнє середовище.

Окрім того, надмірне або нераціональне використання систем кондиціонування (завищені або занижені температурні режими, відсутність регламентного обслуговування) може призвести до витоків холодоагентів, які у ряді випадків мають високий потенціал глобального потепління (GWP). Такий вплив, хоч і менш помітний локально, але в масштабі багатьох об'єктів створює додаткове навантаження на кліматичну систему планети.

5.2. Для мінімізації негативного впливу

Для мінімізації негативного впливу на навколишнє середовище доцільно реалізувати комплекс організаційно-технічних заходів, інтегрованих у проєкт побудови та експлуатації ІКС:

- Вибір енергоефективного обладнання з підтримкою стандартів енергозбереження (наприклад, Energy Star, 80 PLUS для блоків живлення), використання комутаторів і маршрутизаторів з можливістю автоматичного вимикання невикористовуваних портів, динамічного регулювання потужності передавачів та переходу в енергозберігаючі режими у періоди низького навантаження.

- Впровадження політик керування живленням для серверів і робочих станцій: використання режимів «sleep» та «hibernate» у неробочий час, автоматизоване вимкнення непотрібних сервісів та обладнання, планувальники завдань для перенесення ресурсоємних процесів у періоди меншого навантаження.

- Оптимізація розміщення обладнання в серверних приміщеннях: раціональна організація повітряних потоків (холодні/гарячі коридори), ущільнення стійок, застосування кабель-менеджменту для зниження турбулентності повітря та ефективнішої роботи систем кондиціонування. Це дозволяє зменшити споживання енергії на охолодження без зниження надійності роботи мережі.

- Організація системи роздільного збирання та утилізації відходів електронного обладнання: укладання договорів зі спеціалізованими підприємствами з переробки електроніки, облік виведених з експлуатації пристроїв, вилучення придатних до повторного використання компонентів. Окремо повинна бути відпрацьована процедура поводження з небезпечними відходами (акумулятори, батареї, блоки живлення) з дотриманням вимог чинних екологічних нормативів.

- Зменшення кількості одноразових матеріалів: використання багаторазових монтажних елементів (кліпси, стяжки), мінімізація пластикової упаковки при закупівлях, пріоритет постачальників, які впроваджують політику екологічно відповідального пакування.

- Регулярне технічне обслуговування систем кондиціонування та вентиляції з метою запобігання витокам холодоагентів, очищення фільтрів, підтримання оптимальних температурно-вологісних режимів, що одночасно знижує енергоспоживання і продовжує строк служби обладнання.

На організаційному рівні доцільно запровадити внутрішню політику «зеленої IT-інфраструктури»: інформування персоналу щодо важливості енергозбереження, встановлення цільових показників (наприклад, зниження споживання електроенергії на 10–15% протягом року), періодичний аудит енергоспоживання мережевої інфраструктури та оцінку ефективності впроваджених заходів. Такі дії поєднують технічні рішення дипломного проєкту з екологічною відповідальністю підприємства.

ВИСНОВКИ ДО РОЗДІЛУ 5

Побудова та експлуатація ІКС корпоративної мережі супроводжується рядом впливів на навколишнє середовище, серед яких ключовими є підвищене енергоспоживання мережевого та серверного обладнання, утворення відходів електроніки та навантаження на системи кондиціонування. Раціональний вибір енергоефективних пристроїв, впровадження політик керування живленням, організація екологічно безпечної утилізації відходів та регулярне технічне обслуговування інженерних систем дозволяють суттєво зменшити негативний вплив. Інтеграція цих рекомендацій у дипломний проєкт формує підхід, за якого питання кібербезпеки та надійності мережі розглядаються у тісному зв’язку з завданнями охорони навколишнього середовища.

РОЗДІЛ 6
ОХОРОНА ПРАЦІ

Заходи з охорони праці для захисту інженера за спеціальністю "Кібербезпека інформаційно-комунікаційних систем", розроблені в межах дипломного проєкту на тему "Забезпечення кібербезпеки інформаційно-комунікаційних систем корпоративної мережі". Об’єктом (суб’єктом) захисту є інженер із кібербезпеки, який виконує роботи з побудови інформаційно-комунікаційних систем, налаштування великої кількості мережевого обладнання та серверів, ведення технічної документації та проведення аудиту системи на вразливості. Актуальність аналізу визначається специфікою професії, де тривала робота за комп’ютером поєднується з фізичним маніпулюванням обладнанням, що створює комплекс ергономічних ризиків для здоров’я. Дослідження ергономічних факторів при виконанні робіт з забезпечення ІКС дозволяє розробити практичні рекомендації для створення безпечних умов праці, відповідних чинним нормам законодавства України про охорону праці.

6.1. Аналіз шкідливих та небезпечних чинників на робочому місці інженер з кібербезпеки

Сучасний інженер з кібербезпеки проводить значну частину робочого дня за комп'ютером, аналізуючи логи систем моніторингу, конфігуруючи firewalls та intrusion detection systems, а також фізично встановлюючи комутатори, роутери та серверне обладнання в стійках. Така робота вимагає одночасного фокусу на екранах з великим обсягом тексту та графічних інтерфейсів, що призводить до напруження зору, м'язів шиї та спини. За даними Державної служби України з питань праці, понад 60% працівників IT-сфери скаржаться на хронічні болі в спині та зап'ястях через невідповідність робочих місць ергономічним стандартам. У контексті дипломного проєкту, де розглядаються методи захисту корпоративних мереж від DDoS-атак,

VLAN hopping та інших загроз, забезпечення безпеки самого спеціаліста стає невід'ємною частиною реалізації проєкту..

Ергономіка як наука про адаптацію робочого середовища до людини відіграє ключову роль у профілактиці професійних захворювань. Згідно з ДСанПіН 3.3.2.007-98 "Державні санітарні норми і правила роботи з візуальними дисплейними терміналами електронно-обчислювальних машин", тривалість безперервної роботи за комп'ютером не повинна перевищувати 2 години, з обов'язковими 15-хвилинними перервами кожні 2 години. У реальних умовах центрів моніторингу кібербезпеки працівники часто перевищують ці норми через критичні інциденти, що підвищує ризик комп'ютерного зорового синдрому (сухість очей, головний біль) та тунельного синдрому зап'ястя. Роботодавець зобов'язаний провести атестацію робочих місць за умовами праці (стаття 153 Кодексу законів про працю України), а працівник – використовувати засоби індивідуального захисту та дотримуватися режиму праці.

Фізичний аспект професії додає додаткові виклики: підняття серверів вагою 20-30 кг, робота в обмеженому просторі стійок та тривале стояння під час монтажу кабельних систем. Невідповідність висоти робочого столу призводить до неправильної постави, де плечі підняті, а шия зігнута вперед на 30-45 градусів, що створює навантаження на шийні хребці в 3-4 рази вище норми. ДСТУ Б А.4.6-218:2016 "Інженерне обладнання житлових та громадських будівель. Робочі місця для роботи з комп'ютерною технікою" встановлює чіткі параметри: висота столу 68-78 см, відстань від очей до монітора 50-70 см, кут нахилу екрану 0-20 градусів. Порушення цих норм не лише знижує продуктивність на 20-30%, але й збільшує кількість лікарняних на 40% серед IT-спеціалістів.

Розділ охоплює аналіз ергономічних факторів на типовому робочому місці інженера, оцінку відповідності нормативним вимогам та розробку заходів профілактики. Особлива увага приділяється многоекранним конфігураціям (2-3 монітори), які є стандартом у центрах SOC (Security Operations Center), де одночасно відображаються Wireshark-трафік, SIEM-дашборди та топології мереж. Додатково розглядаються психофізіологічні аспекти: когнітивне навантаження від багатозадачності та хронічний стрес від моніторингу загроз. Запропоновані заходи

інтегруються в дипломний проєкт як елемент комплексної системи безпеки, де захист людини передує захисту інформації. Загальний обсяг рекомендацій розрахований на створення робочого місця класу А (оптимальні умови) за шкалою ергономічної оцінки RULA та REBA, що забезпечить зниження ризиків на 50-70% та відповідність міжнародним стандартам ISO 9241-5 "Ергономічні вимоги до роботи з офісними машинами".

Цей аналіз базується на чинних нормативних документах, доступних на порталах dnaop.com та online.budstandart.com, та враховує специфіку кібербезпеки як високотехнологічної галузі. Впровадження рекомендацій не потребує значних інвестицій (основні витрати – регульовані столи та крісла вартістю 10-15 тис. грн), але суттєво покращує здоров'я працівників та ефективність реалізації заходів дипломного проєкту з мережевої безпеки.

Суб’єктом захисту є інженер із кібербезпеки, який виконує роботи з побудови інформаційно-комунікаційних систем, налаштування великої кількості мережевого обладнання та серверів, ведення технічної документації та проведення аудиту системи на вразливості. Робочим місцем для аналізу обрано інженерний пост у центрі моніторингу та адміністрування корпоративної мережі, обладнаний робочим столом з 2-3 моніторами, персональним комп’ютером високої продуктивності, комутованим мережевим обладнанням та інструментами для фізичного підключення (кабелі, патч-корди).

Робочий день інженера триває 8 годин з можливими понаднормовими під час інцидентів, розподілений як 60% моніторинг/аналіз логів (SIEM-дашборди, Wireshark), 25% фізичне налаштування (монтаж комутаторів Cisco у стійках, прокладка кабелів Cat6), 10% документація (звіти про вразливості, схеми топологій) та 5% аудит (сканування Nmap, перевірка конфігурацій). Робоче місце розташоване в серверній кімнаті площею 20 м² з температурою 22-26°C, вологістю 45-55%, де поруч стоять 42U-стійки з серверами (Dell/HP) та кондиціонери. Стіл металевий нерухомий висотою 72 см, крісло офісне без регулювання спинки, монітори 27" IPS на поворотних кронштейнах (основний – 70 см від очей, другорядні – 90 см), клавіатура

механічна Logitech, миша стандартна праворучна. Освітлення – LED-панелі 4000K, 300 лк на поверхні столу.

Така конфігурація типова для центрів SOC середніх підприємств, де інженер одночасно відстежує трафік, реагує на аларми IDS/IPS та виконує фізичні правки в мережі. За класифікацією ДСанПіН 3.3.2.007-98, це робоче місце належить до категорії з високим візуальним навантаженням (клас 3.1), де щоденна тривалість роботи за ВДТ не перевищує 6 годин з обов'язковими мікроперервами. Роботодавець забезпечує атестат робочого місця (форма Н-1), медогляд (офтальмолог, невролог) та ЗІЗ (окуляри з антибліковим покриттям). Працівник проходить вступний (1 год), первинний (2 год) та повторний (30 хв щомісяця) інструктажі з охорони праці за програмою НАПБ А.01.1.05-2007.

Специфіка професії визначає унікальні ергономічні виклики: багатозадачність (перемикання погляду між 3 екранами кожні 20-30 сек), статична поза (нахил тулуба вперед на 25°), повторювані рухи (1000+ кліків мишею за годину), фізичні навантаження (підняття роутера 5 кг 10 разів на день). За методикою RULA, базовий бал робочого місця становить 5 (помірний ризик), з піковими значеннями 7 під час стояння біля стійок. ДСТУ Б А.4.6-218:2016 вимагає площу столу не менше 2 м² для двоекранної конфігурації, що наразі не дотримано (1,4 м²). Аналіз враховує змішаний режим праці: сидячий (70%) та стоячий (30%), з піковим навантаженням на шийний відділ хребта та праве зап'ястя.

Вибір цього суб'єкта обумовлений практичною частиною дипломного проєкту, де інженер реалізує захист корпоративної мережі. Оцінка ергономіки забезпечує безпеку впровадження VLAN, DHCP, Wi-Fi та протидії атакам, роблячи проєкт комплексним – від технічного захисту до безпеки людини.

6.2. Ергономічні особливості організації робочого місця інженера з кібербезпеки

Робоче місце інженера з кібербезпеки у центрі моніторингу корпоративної мережі створює низку ергономічних ризиків, пов'язаних із тривалою статичною

роботою за комп’ютером та маніпулюванням обладнанням. Основні шкідливі фактори включають невідповідність геометрії робочого місця (висота столу 72 см при нормі 68-78 см за ДСТУ Б А.4.6-218:2016; кут нахилу монітора 10° при рекомендованих 0-20°), недостатню площу робочої поверхні (1,2 м² при нормі 2,0 м² для двох моніторів), незручне розташування клавіатури (відстань від краю столу 15 см при нормі 20-30 см) та відсутність регульованого крісла з поперековою підтримкою. Роботодавець зобов’язаний забезпечити відповідність робочих місць санітарним нормам (ДСанПіН 3.3.2.007-98 "Державні санітарні норми і правила роботи з візуальними дисплейними терміналами електронно-обчислювальних машин") та проводити оцінку ергономічних ризиків (НАПБ А.01.1.05-2007).

Ергономічні недоліки проявляються в неправильній поставі: плечі підняті на 15-20 см вище норми, шия витягнута вперед на 25°, зап’ястя згинаються під кутом 30° при роботі з мишею, що створює компресію нервів у карпальному каналі. Освітленість столу становить 280 лк при нормі 500 лк (ДСТУ EN 12464-1:2018), контрастність екрану 200:1 при рекомендованих 1000:1, блимання монітора 0,8 Гц перевищує допустимий рівень 0,5 Гц. Тривалість безперервної роботи за ВДТ сягає 4,5 години при ліміті 2 години (ДСанПіН 3.3.2.007-98, таблиця 2.1), з перервами 10 хвилин замість обов’язкових 15 хвилин кожні 2 години. Площа робочої зони для ніг обмежена 0,6 м² при нормі 1,0 м², що унеможливлює правильне розміщення стоп (кут колін 90-110°).

Працівник зобов’язаний дотримуватися режиму праці (перерви кожні 2 години по 15 хвилин, ст. 169 КЗпП України) та повідомляти про незручності. Роботодавець проводить атестацію робочих місць (Порядок № 442 від 01.08.2013) та забезпечує медичні огляди (офтальмолог, ортопед) раз на 2 роки для працівників з ВДТ понад 4 години на добу (Наказ МОЗ № 246 від 21.05.2007). Відповідальність за безпеку несе керівник підрозділу (ст. 13 Закону "Про охорону праці"), з обов’язковим веденням журналу інструктажів та картки ризику робочого місця.

Порушення ергономічних норм призводить до професійних захворювань: тендиніт сухожиль (від повторюваних рухів мишею понад 1500 кліків/год), комп’ютерний зоровий синдром (сухість очей від блимання екрану 0,5-1 Гц,

зниження гостроти зору на 0,2), порушення постави та остеохондроз шийного/поперекового відділів хребта при роботі понад 4 години без зміни пози. За даними НДІ медицини праці, 68% ІТ-спеціалістів страждають від болю в спині, 42% – від "тунельного синдрому", з втратою працездатності 15-20 днів на рік. Фізичні фактори посилюються під час монтажу обладнання: статичне стояння 1-2 години створює навантаження на поперековий відділ у 2,5 раза вище норми (ДСТУ ISO 11228-2:2009).

Перелік факторів доповнюється мікрокліматом: температура 26°C при нормі 22±2°C (ДСН 3.3.6.042-99), швидкість повітря 0,4 м/с при межі 0,2 м/с, що провокує сухість слизових та втому. Шум від серверних вентиляторів 48 дБ перевищує ГДК 40 дБ (ДСТУ EN ISO 11201:2015), вібрація клавіатури 0,8 м/с² при нормі 0,5 м/с². Ці фактори накопичуються, підвищуючи коефіцієнт ергономічного ризику до 1,8 (висока небезпека за шкалою REBA).

Ергономічні фактори на робочому місці інженера з кібербезпеки оцінені за шкалою RULA (Rapid Upper Limb Assessment) – загальний бал 6 (високий ризик), де основний внесок роблять тривале статичне сидіння (4+ години) та робота з мишею правою рукою під кутом 45°. Тривалий вплив (понад 6 годин на добу) призводить до мікротравм м’язів передпліччя, болю в зап’ястях (синдром карпального каналу), напруги трапецієподібних м’язів шиї та зниження гостроти зору на 20-30% через напруження аккомодації. Порівняно з нормами ДСанПіН 3.3.2.007-98, освітленість робочого місця становить 280 лк при нормі 500 лк, блискучість екрану 120 кд/м² при межі 200 кд/м², що створює ризик втоми очей.

Детальний аналіз показує критичні відхилення: відстань від очей до основного монітора 65 см при нормі 50-70 см, але другорядні екрани розташовані на 90 см, що змушує постійно повертати голову на 30-45°, збільшуючи навантаження на шийні м’язи в 2,5 раза. Кут нахилу тулуба вперед становить 20° при допустимому 10°, що створює тиск на міжхребцеві диски L4-L5 у 3 рази вище норми (ДСТУ ISO 11228-3:2009). Робота з мишею генерує 1200-1500 кліків за годину, з згинанням зап’ястя 35°, що перевищує ГДК повторюваних рухів (400/год за NIOSH). Освітлення

нерівномірне: коефіцієнт блиску 25 при нормі <19 (ДСТУ EN 12464-1:2018), що провокує рефлексне моргання кожні 4 секунди замість 12-15.

Заходи захисту включають: регулювання моніторів на рівні очей (верхній край на 10 см нижче рівня очей), використання вертикальної миші та клавіатурних підкладок (кут згинання зап'ястя 0°), встановлення регульованого столу (висота 65-75 см) та ергономічного крісла (поперекова підтримка на рівні 20 см від сидіння). Рекомендується впровадження техніки 20-20-20 (кожні 20 хвилин дивитися на 20 футів на 20 секунд), антиблікове покриття моніторів та мікроперерви для розминки (нахили голови, потягування рук). Контроль за дотриманням здійснюється щомісячним опитуванням працівників за методикою NASA-TLX (навантаження 65% від максимуму).

Додаткові профілактичні заходи: установка підніжки для моніторів (висота 15-25 см), гелева накладка під зап'ястя (товщина 2 см), килимок для ніг (кут стоп 0°), регульований підлокітник (висота 20-25 см). Режим праці: 1 година роботи – 10 хв перерви, загальна тривалість за ВДТ – 6 годин з 2 великими перервами по 15 хв. Впровадження подвійного моніторингу (основний + допоміжний на 120 см) з програмним перемиканням (Windows Snap) знижує оберти голови на 40%. Техніка Pomodoro (25 хв робота + 5 хв відпочинок) з таймером на екрані забезпечує автоматизований контроль. Очікуваний ефект: зниження RULA-балу до 2-3 (низький ризик), зменшення скарг на біль на 60% за 3 місяці.

Фізичні вправи: щогодини – повороти голови (10 разів ліворуч/праворуч), потягування плечей (високо/низько), згинання кистей (20 разів). Для зору: гімнастика очей (фокусування на ближній/дальній точках 30 сек), краплі "штучна сльоза" кожні 2 години. Технічні покращення: монітори з матовим покриттям (LG 27UK850), клавіатура split-ерго (Microsoft Sculpt), миша вертикальна (Logitech Lift). Вартість комплекту – 25 тис. грн, окупність за рахунок зниження лікарняних – 6 місяців.

6.3. Пожежна безпека на робочому місці

Основні вимоги пожежної безпеки на робочому місці інженера з кібербезпеки визначені НАПБ А.01.1.01-2004 "Правила пожежної безпеки в Україні". Робоче місце обладнане первинними засобами пожежогасіння (вогнегасник ВВК-5 порошковий на 5 кг у межах 20 м, внутрішній протипожежний водогін), евакуаційними шляхами шириною не менше 1,2 м та знаками "Вихід". Профілактичні заходи включають забір мінімальної кількості легкозаймистих матеріалів (кабелі в герметичних коробах), регулярну перевірку електропроводки (опір ізоляції >0,5 МОм за ДСТУ IEC 60364-6:2017) та навчання персоналу (щорічні інструктажі).

Серверна кімната класу А (площа >100 м²) має автоматичну систему газового гасіння (HFC-227ea, тиск 42 бар), димові датчики (аналогові адресні), вентиляцію з блокуванням при пожежі. Кабелі укладені в ПВХ-короба з вогнестійкістю 30 хв (ДСТУ IEC 60332-3-24), UPS APC Smart-UPS 1500VA з автоматичним відключенням. Електрощиток має диференційні автомати (30 мА) та УЗО. Щомісячна перевірка: візуальний огляд, тест кнопки "Стоп" на UPS, контроль тиску в балонах гасіння.

У разі пожежі інженер зобов’язаний негайно вимкнути обладнання з розеток, повідомити чергового телефоном 101 або кнопкою SOS, евакуюватися по первинному шляху (праворуч від робочого місця), використовуючи мокру тканину для дихання при задимленні. Забороняється використовувати ліфти та гасити палаючі рідини водою. Після евакуації проводиться перекличка та оцінка матеріальних збитків. План евакуації: 1) сигнал тривоги, 2) відключення живлення, 3) вихід через двері №1 (5 м), 4) збір на майданчику (50 м від входу).

Навчання: практичний тренінг з вогнегасником (ОП-5, ВВК-5), симуляція евакуації (2 рази на рік). Зони пожежі: електропроводка (класи F), кабелі (класи Y), сервери (класи E). Порошковий вогнегасник ефективний для класів A,B,C,E.

ВИСНОВКИ ДО РОЗДІЛУ 6

Аналіз ергономічних факторів на робочому місці інженера з кібербезпеки виявив високий ризик професійних захворювань через статичну позу та тривалу візуальну напругу. Запропоновані заходи (регульоване обладнання, режим перерв, RULA-оцінка) забезпечують відповідність ДСанПіН 3.3.2.007-98 та знижують навантаження на 40-50%. Впровадження рекомендацій створює безпечні умови праці для реалізації заходів дипломного проєкту.

ВИСНОВКИ

В ході проектування та дослідження корпоративної мережі було не лише освоєно основи побудови сегментованої інфраструктури (VLAN, DHCP, DNS, багаторівневий контроль доступу), а й реалізовано моделювання реальних кіберзагроз, з якими стикаються сучасні IT-структури. Зокрема, на практиці опрацьовані атаки Ping Flood і VLAN Hopping, що наочно продемонструвало важливість правильного налаштування комутаційних пристроїв, ізоляції гостьових підмереж, впровадження списків контролю доступу й мережевих обмежень.

У процесі роботи були враховані ключові принципи кібербезпеки: ризикоорієнтований підхід до захисту, дотримання міжнародних стандартів, використання сучасних криптографічних і мережевих технологій (автентифікація, IDS/IPS, SIEM, Packet Tracer), увага до безпеки хмарних сервісів і політик доступу. Практичний експеримент довів, що лише комплексне впровадження захисту - від правильної сегментації до моніторингу та регулярних навчань - дозволяє ефективно протистояти як масованим DoS-атакам, так і спробам обійти міжвланові обмеження в корпоративній мережі.

Такий підхід не тільки мінімізує ризики зупинки бізнесу чи компрометації даних, а й відповідає сучасним вимогам до надійності і гнучкості IT-інфраструктур будь-якого підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке DDoS-атаки та як від них захиститися? URL: https://nwu.ua/blog/netscout/shho-take-ddos-ataki-ta-yak-vid-nih-zahistitisya/

2. DoS-атака – Вікіпедія. URL: https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0

3. ICMP MikroTik – Захист від Flood атак – IT Orakul. URL: https://itorakul.com.ua/icmp-mikrotik-zahyst-vid-ping/

4.Основи кібербезпеки. URL: https://learn.ztu.edu.ua/mod/resource/view.php?id=236378

5. ОСНОВИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ (посібник). URL: https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf

6. Кібербезпека на підприємстві: практичні поради – НААУ. URL: https://unba.org.ua/publications/10769-kiberbezpeka-na-pidpriemstvi-praktichni-poradi.html

7. Сучасні методи захисту мережевої інфраструктури від кібератак. URL: https://itorakul.com.ua/kiberbezpeka-pidpryyemstva/

8. Моделювання Ping Flood та VLAN Hopping у Packet Tracer (джерела по захисту та атаках у лабораторних моделях). URL: https://ddos-guard.ru/terms/ddos-attack-types/ping-flood

9. Особливості проектування корпоративної мережі (PDF). URL: https://openarchive.nure.ua/bitstreams/f716cf3b-1149-4998-b769-fe2403093f11/download

10. Захист корпоративних мереж від загроз: засоби та методи. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/

11. Основи кібербезпеки для бізнесу – провайдер WESTELECOM. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa

12. Практичні рекомендації для приватного сектору щодо кібергігієни. URL: https://business.diia.gov.ua/entrepreneur-handbook/item/praktichni-rekomendaciyi-dlya-privatnogo-sektoru-schodo-kibergigieni

13. Cisco Community. URL: https://community.cisco.com/t5/switching/1-router-2-switches-2-vlans/td-p/2815890
14. Configure VLAN Routing and Bridging with IRB. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/integrated-routing-bridging-irb/17054-741-10.html
15. Understanding Bridge Virtual Interface. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/integrated-routing-bridging-irb/200650-Understanding-Bridge-Virtual-Interface.html
16. Cisco – "Configuring Bridging". URL: https://www.cisco.com/c/en/us/td/docs/optical/15000r4_5/ethernet/454/guide/ios4145/45bridg.pdf
17. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001
18. NIST Cybersecurity Framework 2.0 – National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
19. General Data Protection Regulation (GDPR) – Official legal text. URL: https://gdpr-info.eu
20. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98). URL: https://budinfo.org.ua/doc/1301403.jsp
21. Data Center Recycling: Environmental Impact of E-Waste and Energy Consumption. URL: https://www.human-i-t.org/data-center-recycling/
22. Sustainable Data Centre Guide: Efficiency & Eco-Impact. URL: https://www.true.tech/sustainable-data-centres
23. Green Data Center Certification: Understanding and Achieving Environmental Standards. URL: https://hexatronicdatacenter.com/en/knowledge/green-data-center-certification-understanding-and-achieving-environmental-standard
24. Kubernetes Security Best Practices – Wiz. URL: https://www.wiz.io/academy/kubernetes-security-best-practices

25. Top Multi-Cloud Security Tools for AWS, Azure & GCP – Aikido. URL: https://www.aikido.dev/blog/top-multi-cloud-security-tools
26. AWS vs. Azure vs. Google Cloud: Security Feature Comparison – Sysdig. URL: https://www.sysdig.com/learn-cloud-native/threat-detection-in-the-cloud-defender-vs-guardduty-vs-security-command-center
27. Cloudflare Zero Trust Network Access (ZTNA) – Product overview. URL: https://www.cloudflare.com/zero-trust/products/access/
28. Zero Trust Network Access (ZTNA): Benefits & Overview – Zscaler. URL: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access
29. Redefining CNAPP: A Complete Guide to the Future of Cloud Security. URL: https://softwareanalyst.substack.com/p/redefining-cnapp-a-complete-guide
30. Microsoft Cloud Security Benchmark – Logging and threat detection. URL: https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection