МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС–КОЛЕДЖ

Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

«ЗАХИСТ ВІД ВНУТРІШНІХ ТА ЗОВНІШНІХ ЗАГРОЗ В ЛОКАЛЬНИХ МЕРЕЖАХ»

Виконав: студент групи 2К–21

Спеціальності

123 «Комп’ютерна інженерія»

Владислав КОВАЛЬЧУК

Керівник:

Павло РАТАЙЧУК

Черкаси 2025

Анотація

У сучасному цифровому середовищі локальні мережі (LAN) відіграють ключову роль в організації обміну інформацією та функціонуванні IT–інфраструктури. Однак з активним розвитком технологій зростає і кількість загроз, спрямованих на порушення їхньої безпеки. Забезпечення ефективного захисту локальних мереж від внутрішніх і зовнішніх загроз є важливим завданням для будь–якої організації.

У кваліфікаційній роботі здійснено комплексний аналіз загроз для локальних мереж. Проведено класифікацію загроз на внутрішні (навмисні або випадкові дії користувачів, витоки інформації, зловживання правами доступу) та зовнішні (мережеві атаки, віруси, фішинг, несанкціонований доступ). Розглянуто архітектуру локальних мереж та ключові вразливості її компонентів.

Проаналізовано сучасні інструменти забезпечення безпеки, такі як IDS/IPS–системи, аналіз трафіку (DPI, NetFlow, Wireshark), технології контролю доступу (RBAC, ACL), SIEM–рішення та інші засоби, зокрема VLAN, VPN, брандмауери, WPA3 і 802.1X. Окрему увагу приділено захисту від соціальної інженерії та застосуванню хмарних сервісів безпеки.

У практичній частині роботи змодельовано атаки, протестовано вплив загроз на мережу та оцінено ефективність захисних механізмів. На основі результатів сформульовано практичні рекомендації з урахуванням технічних, організаційних та економічних аспектів.

Дослідження підтверджує важливість багаторівневого підходу до захисту LAN, який поєднує технічні засоби, політики безпеки та навчання персоналу. Результати можуть бути використані фахівцями з кібербезпеки та адміністраторами мереж для вдосконалення захисту IT–інфраструктур.

Ключові слова: локальні мережі, інформаційна безпека, внутрішні загрози, зовнішні загрози, IDS/IPS, контроль доступу, Zero Trust, SIEM, фішинг, аналіз трафіку, VPN, хмарні рішення, кіберзахист.

Abstract

In the modern digital environment, local area networks (LANs) play a key role in organizing information exchange and functioning of IT infrastructure. However, with the active development of technologies, the number of threats aimed at violating their security is also increasing. Ensuring effective protection of local networks from internal and external threats is an important task for any organization.

The qualification work carried out a comprehensive analysis of threats to local networks. The threats were classified into internal (intentional or accidental user actions, information leaks, abuse of access rights) and external (network attacks, viruses, phishing, unauthorized access). The architecture of local networks and the key vulnerabilities of its components were considered.

Modern security tools were analyzed, such as IDS/IPS systems, traffic analysis (DPI, NetFlow, Wireshark), access control technologies (RBAC, ACL), SIEM solutions and other tools, including VLAN, VPN, firewalls, WPA3 and 802.1X. Special attention is paid to protection against social engineering and the use of cloud security services.

In the practical part of the work, attacks were simulated, the impact of threats on the network was tested, and the effectiveness of protective mechanisms was assessed. Based on the results, practical recommendations were formulated taking into account technical, organizational, and economic aspects.

The study confirms the importance of a multi–level approach to LAN protection, which combines technical means, security policies, and personnel training. The results can be used by cybersecurity specialists and network administrators to improve the protection of IT infrastructures.

Keywords: local networks, information security, internal threats, external threats, IDS/IPS, access control, Zero Trust, SIEM, phishing, traffic analysis, VPN, cloud solutions, cyber security.

Зміст

ВСТУП

Актуальність обраної теми. У сучасному цифровому світі локальні мережі (LAN) є фундаментальною частиною IT–інфраструктури більшості підприємств, установ та організацій. Вони забезпечують обмін даними, доступ до сервісів, управління ресурсами та взаємодію між користувачами. Проте, з поширенням цифрових технологій та збільшенням кількості кіберзагроз, безпека локальних мереж стає критично важливою. Зловмисники активно використовують як зовнішні методи вторгнення, так і внутрішні вразливості, включаючи людський фактор. Це обумовлює необхідність глибокого аналізу загроз та впровадження надійних методів захисту.

Об’єкт дослідження. Об’єктом дослідження є локальні комп’ютерні мережі, які використовуються в організаціях для передачі, зберігання та обробки інформації.

Предмет дослідження. Предметом дослідження є внутрішні та зовнішні загрози безпеці локальних мереж, а також сучасні технічні та програмні засоби їх виявлення і нейтралізації, включаючи системи IDS/IPS, SIEM, VPN, брандмауери та інші засоби мережевого захисту.

Мета дослідження. Метою цієї роботи є дослідження внутрішніх та зовнішніх загроз, що виникають у локальних мережах, аналіз ефективності існуючих методів захисту, а також формування практичних рекомендацій щодо забезпечення комплексної безпеки LAN.

Завдання дослідження. Для досягнення поставленої мети було сформульовано такі основні завдання:

- дати загальну характеристику локальних мереж та виявити основні їхні вразливості;
- класифікувати типи загроз на внутрішні та зовнішні, охарактеризувати їх особливості та методи реалізації;
- проаналізувати сучасні засоби виявлення та захисту від загроз, зокрема IDS/IPS, SIEM, ACL, VLAN, VPN, Firewall тощо;

– змоделювати типові атаки на локальні мережі з метою оцінки ефективності захисних механізмів;

– надати рекомендації щодо підвищення рівня інформаційної безпеки з урахуванням технічних і організаційних чинників.

РОЗДІЛ 1
АНАЛІЗ ЗАГРОЗ ДЛЯ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Загальна характеристика локальних мереж (LAN)

Локальна комп’ютерна мережа (LAN) – це сукупність комп’ютерів та інших пристроїв, з’єднаних каналами передавання даних у межах обмеженої території (офісу, школи, будинку) для спільного використання апаратних, програмних та інформаційних ресурсів під керуванням спеціального мережевого програмного забезпечення[1].

Основне призначення локальної мережі – забезпечити:

- швидкий обмін даними між пристроями,
- спільний доступ до периферійних пристроїв (наприклад, принтерів, сканерів),
- віддалене керування комп’ютерами.

У такій мережі комп’ютери можуть виконувати різні ролі:

- сервер – керує ресурсами мережі та надає їх у спільне користування
- клієнт (робоча станція) – користується цими ресурсами.

1.2 Основні вразливості локальних мереж

Локальні комп’ютерні мережі, незважаючи на свою ефективність та зручність, мають низку вразливостей, які можуть бути використані зловмисниками для порушення цілісності, конфіденційності або доступності даних. Нижче наведено ключові типи загроз, які варто враховувати під час проектування та експлуатації LAN[2].

Несанкціонований доступ. Одна з найбільш поширених вразливостей можливість стороннього підключення до мережі. Особливо це стосується бездротових мереж Wi–Fi, де слабке або відсутнє шифрування дає змогу підключитися зловмисникам, які перебувають у радіусі дії сигналу. Отримавши

доступ, вони можуть переглядати або змінювати передавані дані, налаштування обладнання чи навіть повністю вивести мережу з ладу.

Слабкі паролі та облікові записи. Використання простих, стандартних або повторюваних паролів для входу до маршрутизаторів, серверів чи інших мережевих пристроїв робить мережу легкою мішенню.

Зловмисники можуть отримати доступ до системи за допомогою перебору (brute force) або використання відомих даних входу.

Відсутність шифрування трафіку. Якщо в мережі не використовується шифрування (наприклад, протокол HTTPS або VPN), передані дані можуть бути легко перехоплені за допомогою спеціальних програм, таких як сніффери. Це стосується як паролів, так і конфіденційної інформації користувачів.

Розповсюдження шкідливого ПЗ. Один інфікований комп'ютер може заразити інші пристрої в мережі. Наприклад, віруси, трояни або програми–шпигуни можуть поширюватися через спільні папки, флеш–накопичувачі або навіть автоматично через відкриті порти.

1.3 Класифікація загроз

Внутрішні загрози – це ризики, які походять безпосередньо від користувачів або пристроїв усередині локальної мережі. Їх складність полягає в тому, що джерело загрози зазвичай має певний рівень довіри в системі. Ці загрози можуть бути як ненавмисними, так і навмисними, і вони часто залишаються непоміченими до моменту виникнення серйозної проблеми[3].

Несанкціонований доступ. Усередині організації працівник може намагатися отримати доступ до ресурсів, які не входять до його службових обов'язків. Це може бути викликано цікавістю, непорозумінням або зловмисними намірами. Наприклад, співробітник без відповідних прав доступу намагається відкрити файли бухгалтерії або адміністративні панелі.

Витік конфіденційної інформації. Навмисне або випадкове розголошення важливої інформації – одна з найнебезпечніших загроз.

Співробітник може передати документи третім особам або помилково відправити конфіденційні дані на зовнішню електронну адресу. Особливо небезпечними є випадки, коли дані потрапляють до конкурентів або зловмисників.

Внутрішні шкідливі програми. Деякі користувачі можуть навмисно встановлювати шкідливе програмне забезпечення, щоб порушити роботу мережі або отримати контроль над системою. Це можуть бути трояни, кейлогери, бекдори та інші типи шкідливого ПЗ, запущені з комп'ютера легального користувача.

Некоректні налаштування та помилки адміністрування Адміністратори або технічні фахівці можуть випадково налаштувати систему таким чином, що з'являються вразливості – наприклад, залишити відкритими порти, не обмежити доступ до мережевих ресурсів або не активувати шифрування.

Зовнішні загрози походять поза меж внутрішньої інфраструктури. Вони зазвичай спрямовані на порушення роботи мережі, викрадення даних або отримання несанкціонованого доступу до ресурсів.

До основних зовнішніх загроз належать:

Атаки DDoS (Distributed Denial of Service) – масовані атаки, що спрямовані на виведення з ладу серверів або мережевих пристроїв шляхом перевантаження їх численними запитами з великої кількості джерел. У результаті справжні користувачі не можуть отримати доступ до ресурсів.

Вірусні та мережеві атаки – включають шкідливе програмне забезпечення (malware), вимагальників (ransomware), а також фішингові атаки. Вони можуть спричинити втрату даних, їх шифрування з подальшою вимогою викупу або крадіжку облікових даних через підроблені сайти чи електронні листи.

Атаки на Wi–Fi та MITM (Man–in–the–Middle) –зловмисники можуть перехоплювати трафік у незахищених або слабо захищених бездротових мережах. У випадку атак типу "людина посередині" вони вбудовуються в

комунікацію між двома сторонами, отримуючи змогу підслуховувати, змінювати або підміняти дані.

SQL–ін'єкції та експлойти – спрямовані на вразливості в програмному забезпеченні. Через SQL–ін’єкції зловмисники можуть отримати доступ до баз даних або модифікувати їх вміст, а за допомогою експлойтів – використовувати вразливості систем або додатків для несанкціонованого доступу або запуску шкідливого коду.

РОЗДІЛ 2
МЕТОДИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ВІД ВНУТРІШНІХ ТА ЗОВНІШНІХ ЗАГРОЗ

2.1 Системи виявлення та запобігання вторгнень (IDS/IPS)

Системи IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) призначені для забезпечення захисту комп’ютерних мереж від зовнішніх і внутрішніх загроз шляхом виявлення, аналізу та реагування на підозрілу активність у трафіку.

IDS – це система виявлення вторгнень, яка аналізує мережевий або системний трафік і повідомляє адміністратора про потенційні загрози. Вона не втручається в трафік, а лише виконує моніторинг та інформування.

IPS – це система запобігання вторгнень, яка не тільки виявляє загрози, але й автоматично блокує або запобігає їхньому виконанню. Вона працює в реальному часі, фільтруючи шкідливі пакети, припиняючи підозрілу активність або закриваючи відповідні з'єднання.

Обидві системи можуть базуватись на сигнатурному методі (порівняння з відомими шаблонами атак) або на поведінковому аналізі (виявлення відхилень від нормальної поведінки системи)[4].

2.2 Аналіз мережевого трафіку (Deep Packet Inspection, NetFlow, Wireshark)

Deep Packet Inspection (укр. глибокий аналіз пакетів) – технологія перевірки та фільтрації пакетів за змістом. На відміну від брандмауера, DPI аналізує не тільки заголовки пакетів, але і їх вміст, відповідно мережевої архітектури моделі OSI, з другого рівня і вище. Deep Packet Inspection здатен виявляти і блокувати віруси, фільтрувати інформацію, відповідно до заданих критеріїв. Deep Packet Inspection може ухвалювати рішення не тільки за вмістом

пакетів, але й за непрямими ознаками, властивим певним мережевим програмами і протоколам. Для цього може бути використаний статистичний аналіз (наприклад, аналіз частоти появи певних символів, довжини пакета тощо). Deep Packet Inspection часто використовують інтернет–провайдери для контролю трафіку, а іноді й для блокування деяких протоколів, таких як BitTorrent. За допомогою Deep Packet Inspection можна визначити, яка програма згенерувала або отримує дані, і на підставі цього виконати певну дію[5].

NetFlow – це протокол від Cisco, що використовується для збору статистики про мережевий трафік. На відміну від DPI, NetFlow не аналізує повний вміст пакетів, а збирає метадані про з'єднання: джерело, призначення, кількість переданих байтів, час з'єднання тощо. NetFlow застосовується для моніторингу продуктивності мережі, виявлення ботнетів, DoS–атак, аномалій у поведінці користувачів[6].

Wireshark – це спеціалізоване програмне забезпечення для аналізу мережевого трафіку, що використовується з метою дослідження, моніторингу та діагностики мережевих протоколів. Програма реалізує функціональність сніффера, тобто інструмента для перехоплення та декодування мережевих пакетів у реальному часі або з файлів, попередньо збережених для подальшого аналізу. Завдяки широкій підтримці протоколів, Wireshark дозволяє здійснювати глибоку інспекцію вмісту кожного окремого пакета, включаючи деталі заголовків, параметри з'єднання, службову інформацію та корисні дані[7].

2.3 Контроль доступу та управління привілеями користувачів (RBAC, ACL)

Модель керування доступом RBAC (Role–Based Access Control) ґрунтується на принципі призначення прав доступу не окремим користувачам, а певним ролям. Кожна роль має чітко визначений набір дозволів, а користувачі отримують ті права, які відповідають їхній ролі. Наприклад, система може включати ролі на кшталт «Адміністратор», «Користувач» або «Гість», кожна з

яких має різний рівень доступу до ресурсів. Такий підхід суттєво спрощує адміністрування, особливо у великих організаціях, де необхідно керувати великою кількістю облікових записів. Крім того, RBAC зменшує ймовірність помилок, пов’язаних із ручним призначенням прав, та сприяє підвищенню загального рівня безпеки, оскільки обмежує надмірні привілеї, надаючи лише ті доступи, які дійсно потрібні користувачу.

ACL – Access Control Lists Списки керування доступом (Списки керування доступом) застосовуються в різних середовищах для точного регулювання прав користувачів до ресурсів. Вони активно використовуються у файлових системах, зокрема NTFS та файлових системах Linux, а також на мережевих пристроях, таких як маршрутизатори й комутатори, де дозволяють визначати, який трафік може проходити через інтерфейси. Крім того, ACL реалізуються в операційних системах і окремих сервісах для забезпечення більш гнучкого контролю над доступом до ресурсів. Основною перевагою цього механізму є можливість тонкого налаштування доступу на рівні окремих користувачів або груп. Водночас, у великих та складних системах управління ACL може виявитися трудомістким, особливо у порівнянні з ролевою моделлю RBAC, оскільки вимагає чіткого відстеження та постійного оновлення окремих правил доступу[8].

2.4 Використання SIEM–систем для моніторингу загроз

SIEM (Security Information and Event Management) – це програмно–апаратний комплекс, який поєднує функції управління інформацією безпеки (SIM) та управління подіями безпеки (SEM). Основне призначення SIEM–систем полягає у виявленні, аналізі та реагуванні на підозрілу активність у комп’ютерних мережах в реальному часі, а також у збереженні журналів подій для подальшого аудиту, розслідувань інцидентів та забезпечення відповідності нормативним вимогам (наприклад, ISO/IEC 27001, GDPR, PCI DSS).

SIEM–система централізовано збирає журнали подій з різноманітних джерел, таких як мережеві пристрої (маршрутизатори, комутатори), сервери, фаєрволи, антивірусні рішення, системи контролю доступу та інші засоби захисту. Отримані дані зберігаються у захищеному середовищі, де здійснюється їхній аналіз та кореляція подій, що дозволяє виявляти складні загрози, які можуть бути непомітними при аналізі окремих подій. Наприклад, якщо виявлено кілька невдалих спроб входу в систему з різних IP–адрес, SIEM може розпізнати це як спробу брутфорс–атаки[9].

Системи SIEM забезпечують моніторинг у реальному часі, а також автоматичне реагування на інциденти: блокування підозрілих дій, створення сповіщень для адміністраторів, ізоляція уражених вузлів або інтеграція з іншими системами безпеки, такими як IDS/IPS. Крім того, SIEM генерує детальні звіти для аналізу та аудиту, включаючи активність користувачів, зміни конфігурацій, спроби несанкціонованого доступу тощо.

У мережевій інфраструктурі SIEM–системи зазвичай розміщуються у ключових точках: на межі мережі для контролю зовнішнього трафіку, у критичних внутрішніх сегментах, де обробляються важливі дані, а також у хмарних середовищах при використанні гібридної архітектури. Це дозволяє покривати увесь периметр мережі та забезпечувати повний контекст подій безпеки.

Завдяки своїм можливостям SIEM–системи забезпечують раннє виявлення загроз, скорочують час реакції на інциденти, дозволяють централізовано керувати інформаційною безпекою та підвищують загальний рівень захищеності організації[[[[[[.

2.5 Технології забезпечення безпеки локальних мереж

Firewall – це програмний або апаратний засіб мережевої безпеки, призначений для контролю вхідного та вихідного мережевого трафіку на основі визначених правил безпеки. Основна функція фаєрвола полягає у фільтрації

пакетів даних між внутрішньою мережею (наприклад, локальною мережею організації або домашньою мережею) та зовнішніми мережами, зокрема Інтернетом, з метою запобігання несанкціонованому доступу, атак або витоку інформації.

Фаєрвол може працювати на різних рівнях мережевої моделі: від простого контролю IP–адрес та портів до аналізу вмісту трафіку (глибока інспекція пакетів). Залежно від типу, фаєрволи поділяють на мережеві (hardware firewall) і програмні (software firewall). Перші зазвичай розміщуються на периферії мережі, виконуючи роль шлюзу, тоді як другі встановлюються безпосередньо на пристроях користувачів або серверах[10].

VLAN (Virtual Local Area Network) – це логічне об'єднання пристроїв у мережі, яке дозволяє хостам взаємодіяти, ніби вони знаходяться в одній локальній мережі, незалежно від їх фізичного розташування. VLAN має ті самі властивості, що й фізична мережа, але дозволяє:

VLAN дозволяє ізолювати трафік між різними групами користувачів для підвищення безпеки, гнучко конфігурувати мережу без фізичного переміщення пристроїв шляхом використання програмного забезпечення, зменшувати навантаження на мережу завдяки поділу широкомовних доменів, а також спрощувати адміністрування та масштабування мережевої інфраструктури.

VPN – це технологія, яка створює захищене, зашифроване з'єднання між користувачем і приватною мережею через Інтернет, дозволяючи бути повноцінним учасником віддаленої мережі навіть поверх загальнодоступних каналів зв'язку. За допомогою шифрування та тунелювання трафіку, VPN забезпечує конфіденційність, цілісність і захист переданих даних[11].

Zero Trust (нульова довіра) – це модель безпеки, яка базується на припущенні, що мережу вже зламано, і нікому не можна довіряти за замовчуванням. Основними її принципами є обов’язкова перевірка кожного запиту доступу, незалежно від його походження – внутрішнього чи зовнішнього, мінімізація привілеїв для користувачів і систем, постійний моніторинг поведінки для виявлення аномалій, а також ретельне управління політиками доступу та

контролем міжмережевих взаємодій. Мета Zero Trust – забезпечити максимально детальний контроль доступу та запобігти несанкціонованому проникненню[12].

WPA3 (Wi–Fi Protected Access 3) – це сучасний стандарт захисту бездротових мереж, що замінив WPA2. Його головною метою є підвищення рівня безпеки навіть при використанні слабких паролів. Завдяки впровадженню протоколу SAE (Simultaneous Authentication of Equals) WPA3 забезпечує покращений захист від атак перебору паролів. Кожен користувач отримує індивідуальне шифрування трафіку, що підвищує конфіденційність, навіть у відкритих Wi–Fi мережах, де сесія шифрується автоматично. Мінімальний рівень шифрування для персонального доступу становить 128 біт, а для корпоративного – 192 біти[13].

802.1X – це протокол контролю доступу, який реалізується за моделлю клієнт–сервер і працює як у дротових, так і бездротових мережах. Його завдання здійснити аутентифікацію користувача або пристрою перед тим, як дозволити повний доступ до мережевих ресурсів. У моделі 802.1X беруть участь три основні компоненти: клієнтський пристрій, що ініціює підключення (Supplicant), точка доступу або комутатор, який блокує або дозволяє доступ (Authenticator), та сервер аутентифікації, зазвичай сервер RADIUS, який перевіряє облікові дані[14].

Захист від соціальної інженерії та фішингу – це набір заходів, що допомагають уникати обману, спрямованого на отримання конфіденційної інформації шляхом маніпуляцій. Такі атаки часто приходять через підроблені листи, сайти чи дзвінки, які імітують довірені джерела[15].

Основні методи захисту:

- Обізнаність користувачів – навчання розпізнавати підозрілу активність.
- Двофакторна автентифікація (2FA) – навіть якщо пароль вкрадено, зловмисник не зможе увійти.
- Перевірка URL – перед введенням даних слід переконатися, що адреса сайту справжня.

– Не відкривати підозрілі вкладення чи посилання – навіть якщо лист виглядає офіційним. Приклад таких листів зображено на Рис. 2.1.

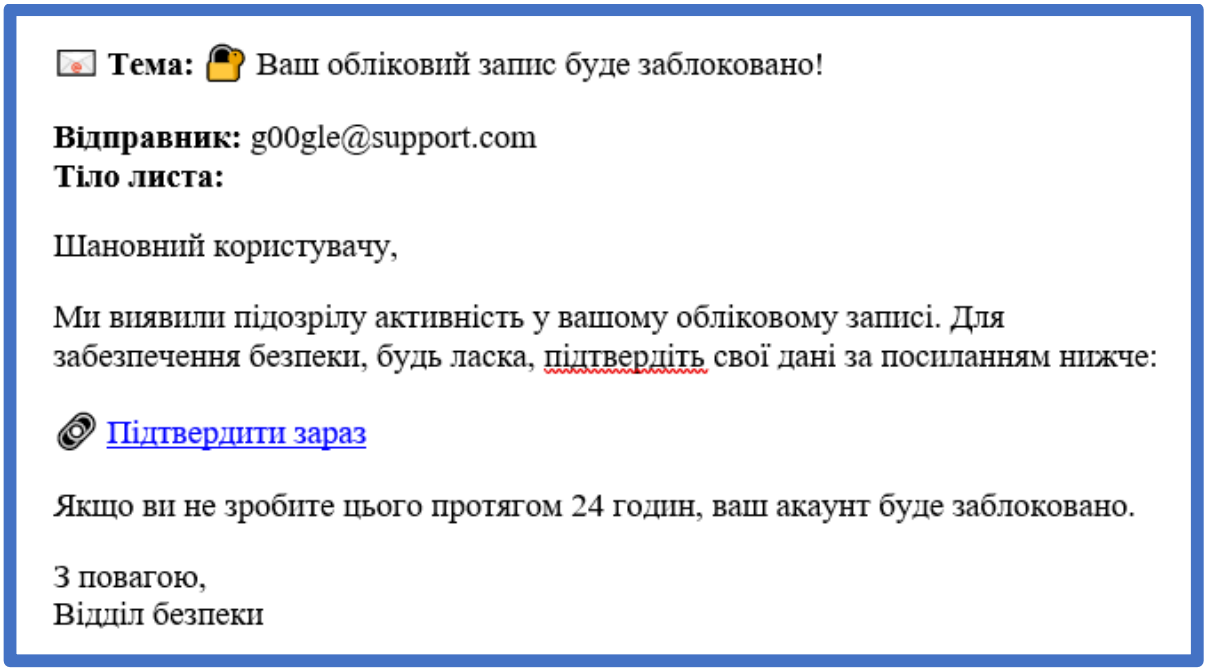

Рисунок 2.1 – Приклад фішингових листів

2.7 Використання хмарних рішень для безпеки мережі (Cloud Firewall, SASE)

Cloud Firewall – це мережевий екран, який функціонує в хмарному середовищі. Він забезпечує фільтрацію вхідного та вихідного трафіку без потреби у фізичному обладнанні, дозволяючи організаціям захищати свої ресурси, розміщені як у хмарі, так і локально. Cloud Firewall дозволяє централізовано керувати політиками доступу, швидко масштабувати захист і зменшувати складність підтримки локальної інфраструктури. Це особливо корисно для розподілених або гібридних IT–середовищ[16].

SASE (Secure Access Service Edge) – це архітектура, яка об’єднує мережеві функції (як-от SD-WAN) з функціями безпеки (зокрема, VPN, контролем доступу, захистом від загроз, firewall–as–a–service) в єдину хмарну платформу[17].

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЗАХИСТУ ЛОКАЛЬНИХ МЕРЕЖ

3.1 Методологія тестування безпеки LAN

Методологія тестування включала кілька етапів: проектування топології, налаштування мережевих пристроїв, впровадження базових сервісів, реалізація захисних механізмів та імітація потенційних загроз. Було розроблено структуру локальної мережі, яка включає кілька сегментів (відділів), об'єднаних за допомогою комутаторів та маршрутизаторів. Налаштовано сервери, серед яких DHCP–сервер для автоматичної видачі IP-адрес, DNS-сервер для доменного іменування, а також HTTP, FTP та Email сервери для забезпечення базових мережевих сервісів.

Для тестування було створено локальну мережу в середовищі Cisco Packet Tracer, що дозволило змоделювати ключові аспекти мережевої інфраструктури та провести базову оцінку її безпеки. Схему створеної мережі наведено на Рис 3.1. У рамках конфігурації мережі було реалізовано сегментацію за допомогою віртуальних локальних мереж (VLAN), що дало змогу розмежувати трафік між окремими логічними групами пристроїв та обмежити їхню взаємодію відповідно до ролей та функцій.

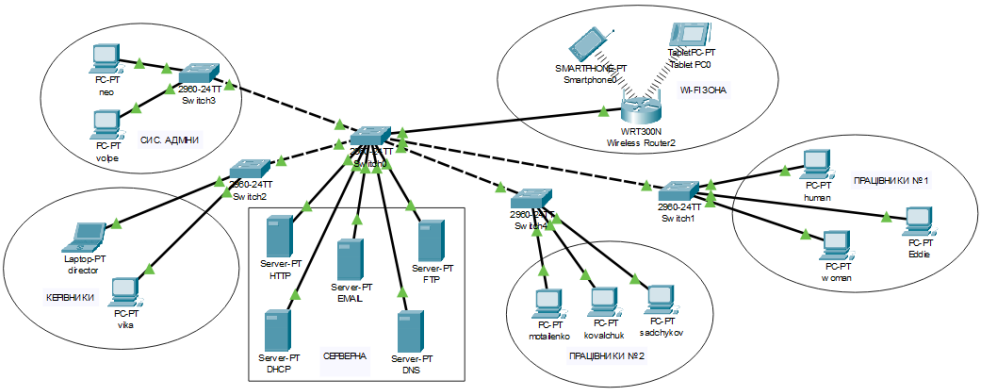

Рисунок. 3.1 – Локальна мережа розроблена для моделювання атаки

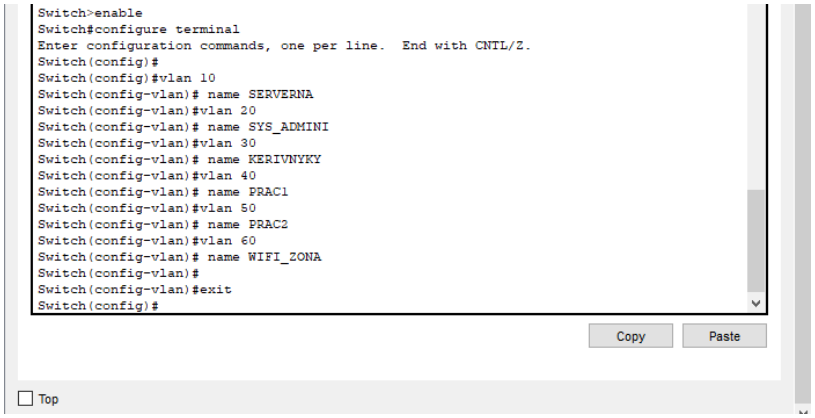

Рисунок 3.2 – Налаштування центрального комутатора: створення VLAN для окремих відділів мережі

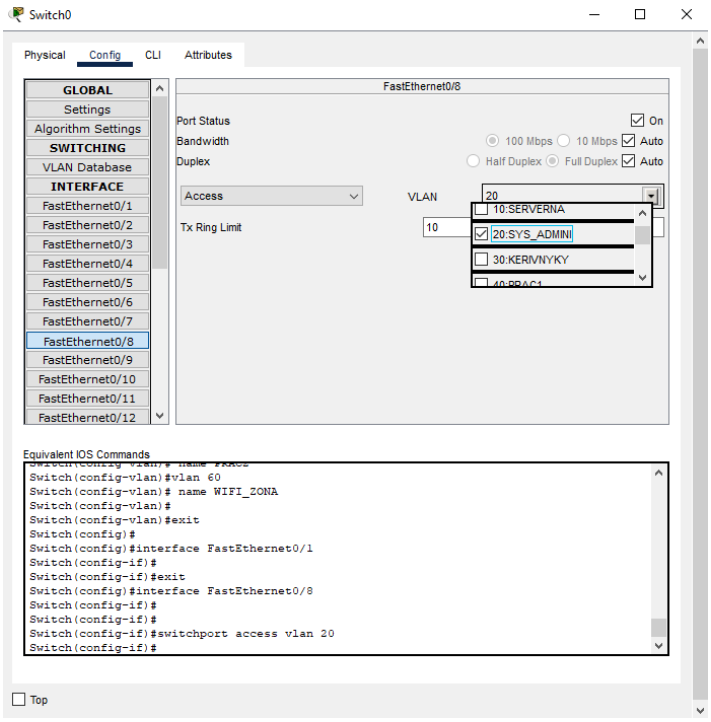

Рисунок 3.3 – Розподіл портів комутатора відповідно до VLAN: призначення фізичних інтерфейсів для окремих сегментів мережі (кабінетів та відділів)

На Рисунках 3.2 та 3.3 представлено процес налаштування портів комутаторів для роботи VLAN.

Після налаштування портів було проведено перевірку коректності взаємодії між пристроями за допомогою команди ping, результати якої наведено на рисунку 3.4.

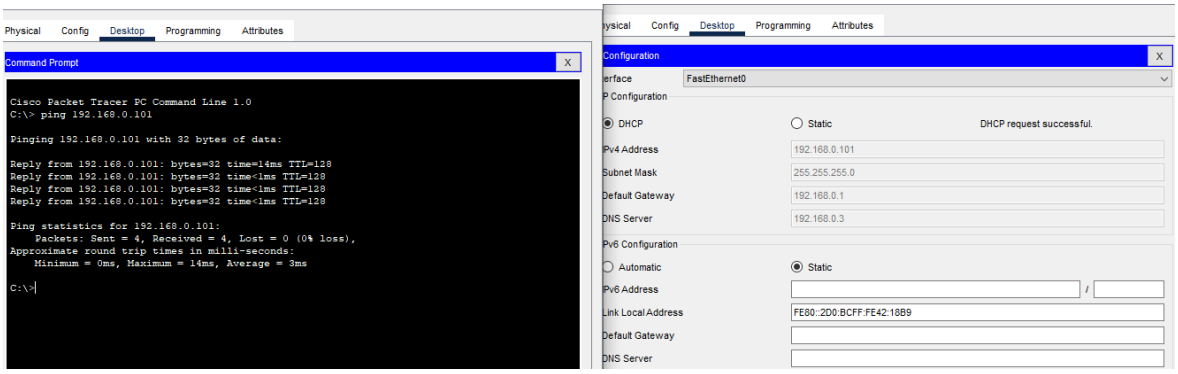

Рисунок 3.4 – Перевірка мережевого з’єднання пристроїв різних VLAN за допомогою команди “ping”

Впроваджено елементи міжмережевого екранування (firewall), яке забезпечує базове фільтрування пакетів і дозволяє контролювати вхідні та вихідні з'єднання відповідно до визначених політик доступу. Схему впровадження ASA наведено на рисунку 3.5. Така конфігурація дозволила імітувати сценарії взаємодії у межах корпоративної мережі з початковим рівнем захисту та заклала основу для подальшого аналізу ефективності впроваджених заходів.

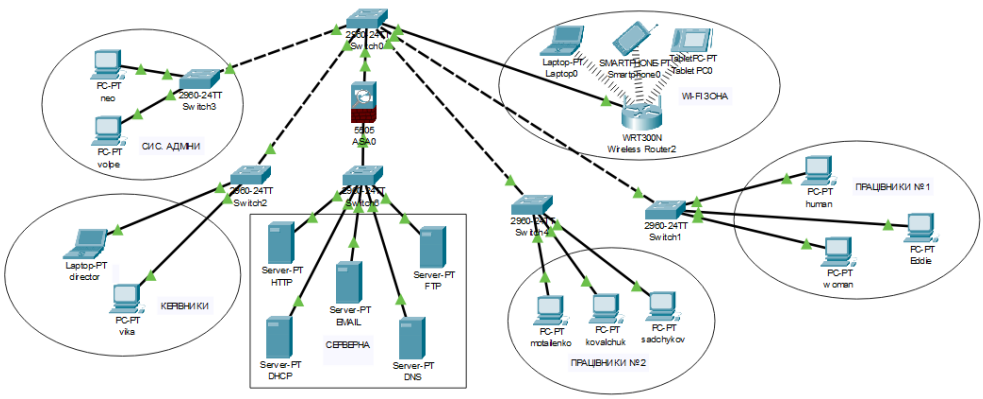

Рисунок 3.5 – Розширення мережі за допомогою міжмережевого екрана ASA для контролю міжвланового трафіку

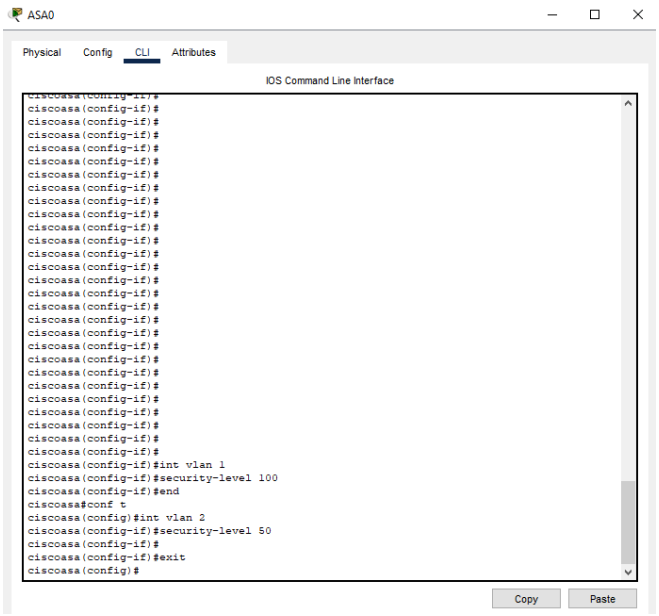

Рисунок 3.6 – Конфігурація рівнів довіри на міжмережевому екрані ASA

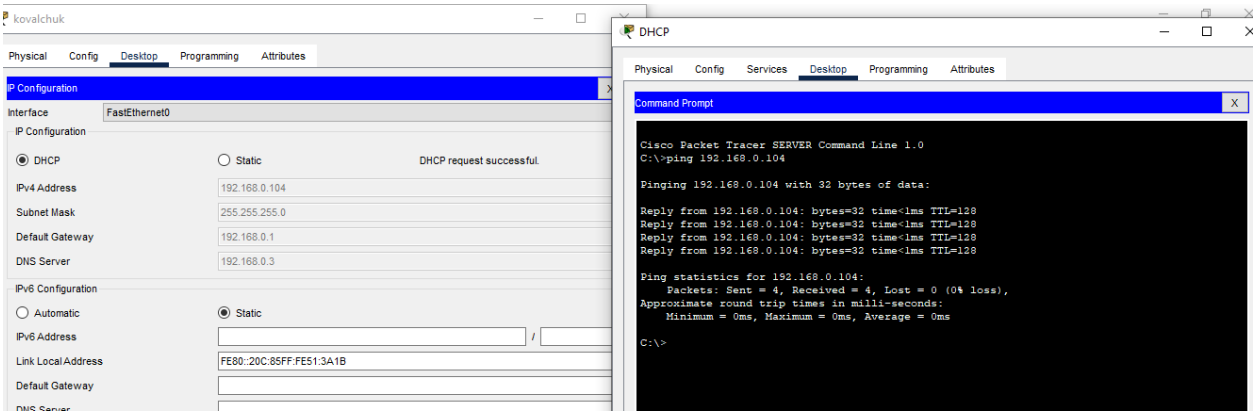

Рисунок 3.7 – Перевірка доступності ПК з сервера через міжмережевий екран ASA

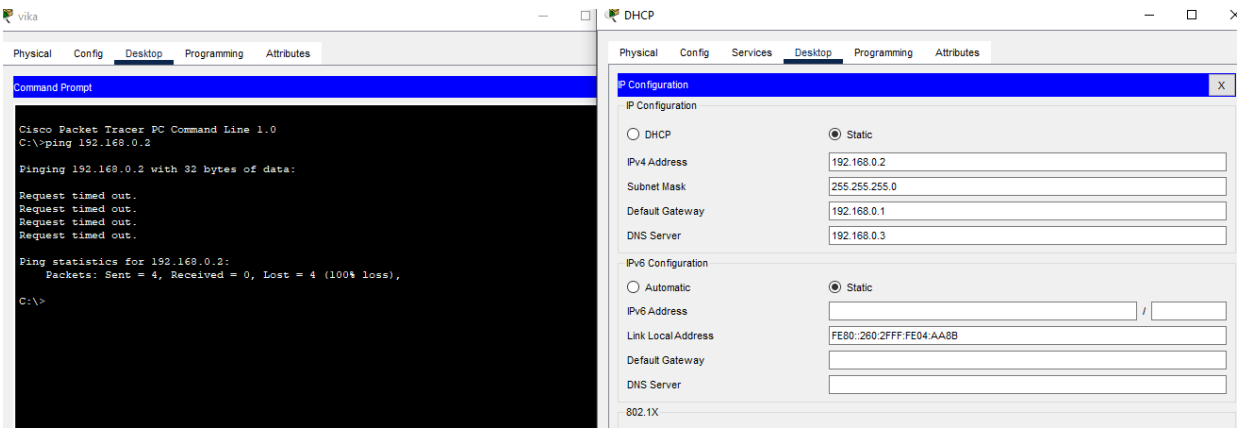

Рисунок 3.8 – Перевірка обмеження доступу: ПК не може пінгувати сервер згідно з налаштованими правилами ASA

Було виконано конфігурацію рівнів довіри на міжмережевому екрані Cisco ASA для розмежування доступу між зонами з різним рівнем безпеки. Після цього проведено перевірку доступності клієнтського ПК із сервера через міжмережевий екран, а також перевірку обмеження доступу — згідно з налаштованими політиками ASA, клієнтський ПК не зміг здійснити ping до сервера. Відповідні результати налаштувань і перевірок наведено на рисунках 3.6–3.8.

Також для забезпечення безпечного віддаленого доступу до корпоративної мережі було впроваджено VPN–тунель, який дозволяє зашифрувати передані дані та гарантує конфіденційність інформації між віддаленими користувачами та внутрішніми ресурсами. Додатково для об'єднання віддалених мереж між різними офісами було налаштовано GRE–тунель, що забезпечує прозоре транспортування мережевого трафіку через публічну інфраструктуру та дозволяє підтримувати логічне з’єднання між сегментами мережі незалежно від фізичного розташування. Використання цих тунелів підвищує загальний рівень безпеки та гнучкість мережевої інфраструктури. Для створення та тестування VPN-з’єднання було змодельовано два офіси. Схематичне зображення мережевої інфраструктури обох офісів наведено на рисунку 3.9.

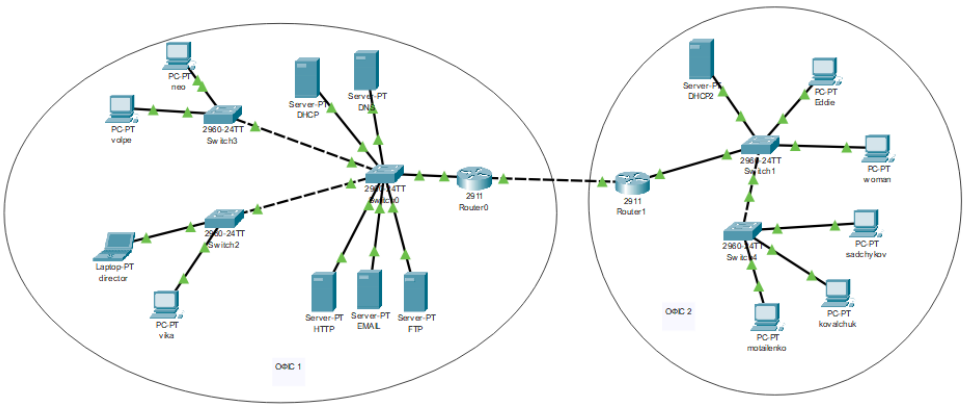

Рисунок 3.9 – Локальна мережа з двома офісами

На рисунках 3.10 та 3.11 показано процес налаштування GRE-тунелю між двома офісами. Продемонстровано конфігурацію інтерфейсів тунелю, а також параметри маршрутизації, які забезпечують коректну передачу даних через захищений канал.

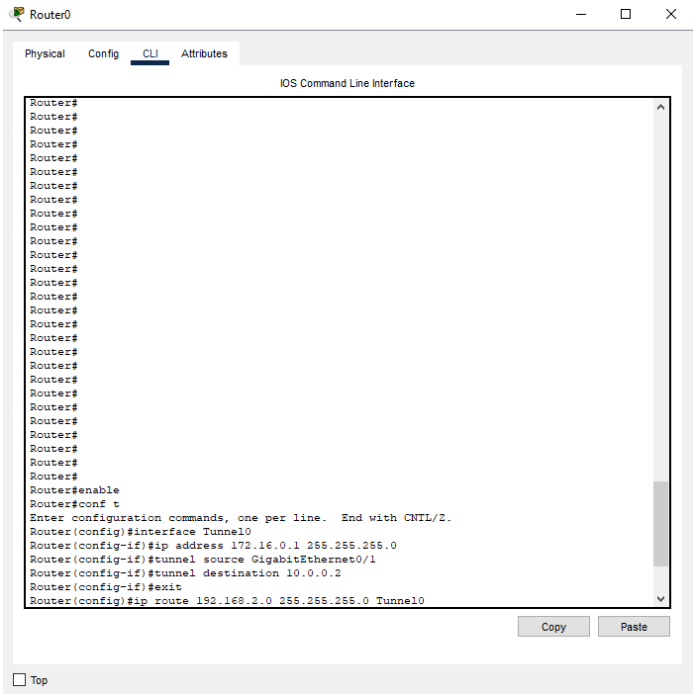

Рисунок 3.10 – Налаштування роутера першого офісу

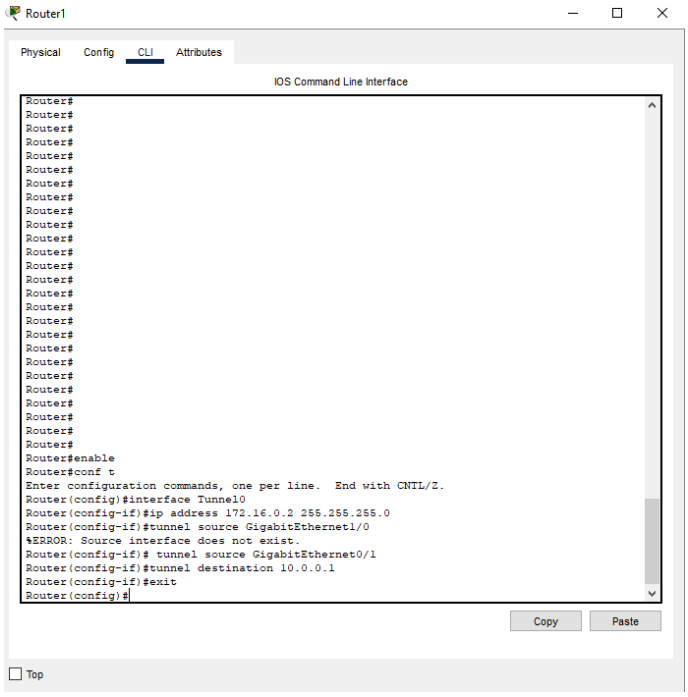

Рисунок 3.11 – Налаштування роутера другого офісу

На Рисунку 3.12 наведено результати перевірки стану інтерфейсів портів та GRE-тунелю, що підтверджують їх коректне функціонування.

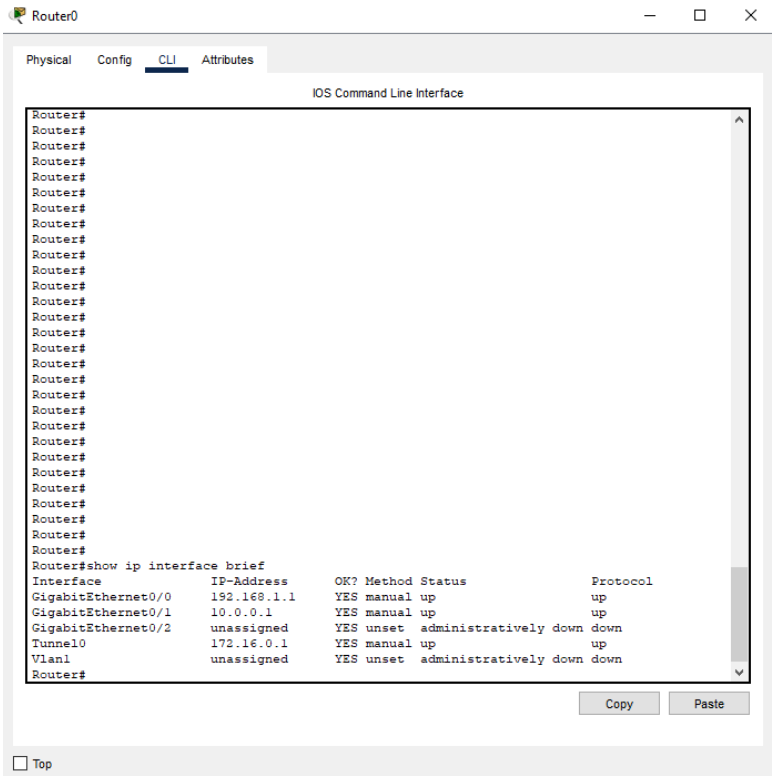

Рисунок 3.12 – Перевірка інтерфейсів портів, та тунелю

На рисунку 3.13 наведено результати перевірки з’єднання між двома офісами через налаштований GRE-тунель, що підтверджують успішну передачу даних і стабільність каналу.

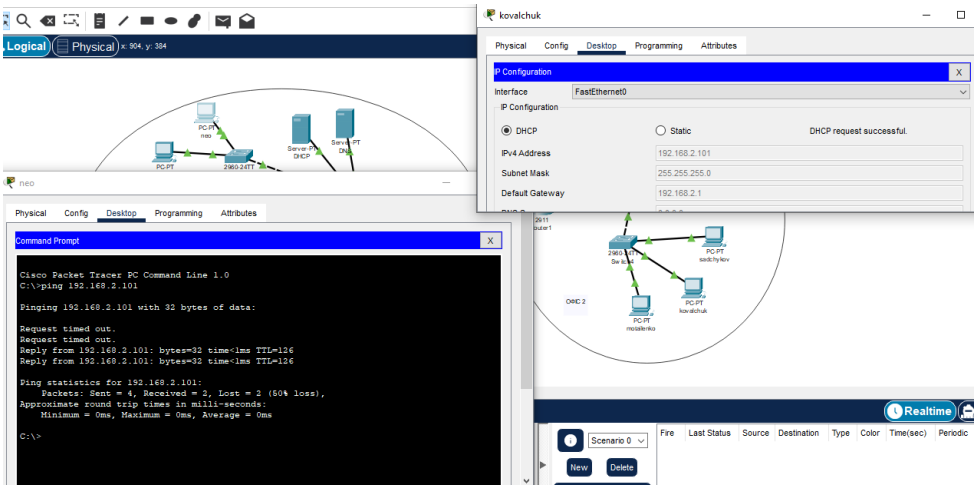

Рисунок 3.13 – Перевірка з’єднання

3.2 Моделювання атак та їх вплив на мережу

У межах можливостей середовища Cisco Packet Tracer буде змодельовано мережеву атаку – DoS (Denial of Service), що імітує перевантаження сервера великою кількістю запитів. Метою є перевірка ефективності базових механізмів захисту та демонстрація того, як такі засоби, як VLAN, Firewall, та VPN впливають на стійкість мережі до поширених загроз. Кожен із варіантів захисту буде реалізовано окремо для порівняння результатів.

Сценарій № 1

У цьому сценарії зловмисник, видаючи себе за клієнта або гостя компанії, підключається до Wi–Fi у зоні для відвідувачів. Перебуваючи в мережі, він починає здійснювати атаки типу DoS, намагаючись порушити нормальну роботу мережевих пристроїв або отримати несанкціонований доступ до внутрішніх ресурсів компанії. Атака проводиться на мережу, організовану за допомогою VLAN, що дозволяє сегментувати мережу і відокремити гостьовий трафік від корпоративного. Процес атаки, у якому атака на клієнта виявилася успішною, наведено на рисунку 3.14. Сценарій імітує реальну ситуацію, коли гостьовий доступ стає точкою входу для потенційної загрози.

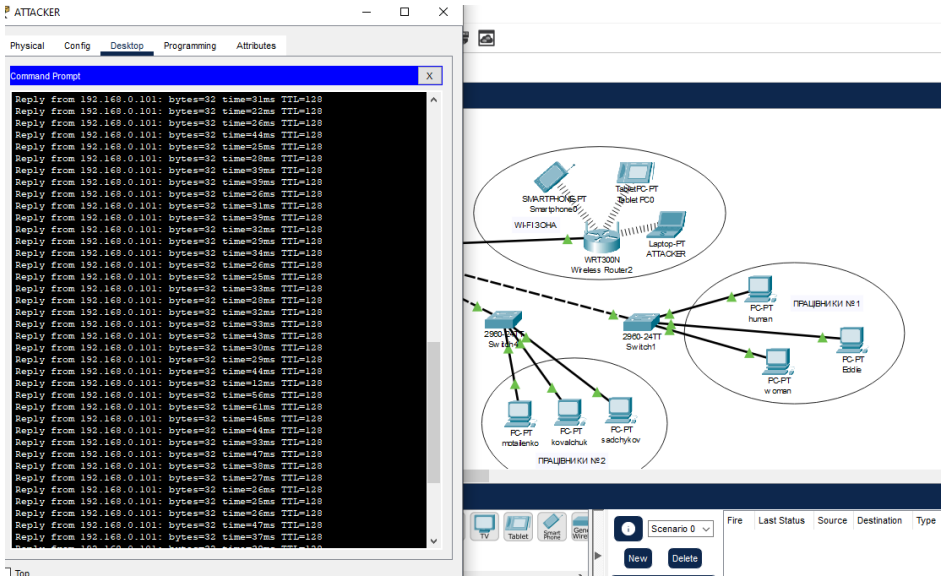

Рисунок 3.14 – Було здійснено DoS–атаку на гостьовий планшет. Атака пройшла успішно з точки зору зловмисника

На рисунку 3.15 показано проведення атаки типу DoS на сервер, проте завдяки реалізації VLAN атаки вдалось запобігти, що підтверджує ефективність сегментації мережі у захисті внутрішніх ресурсів.

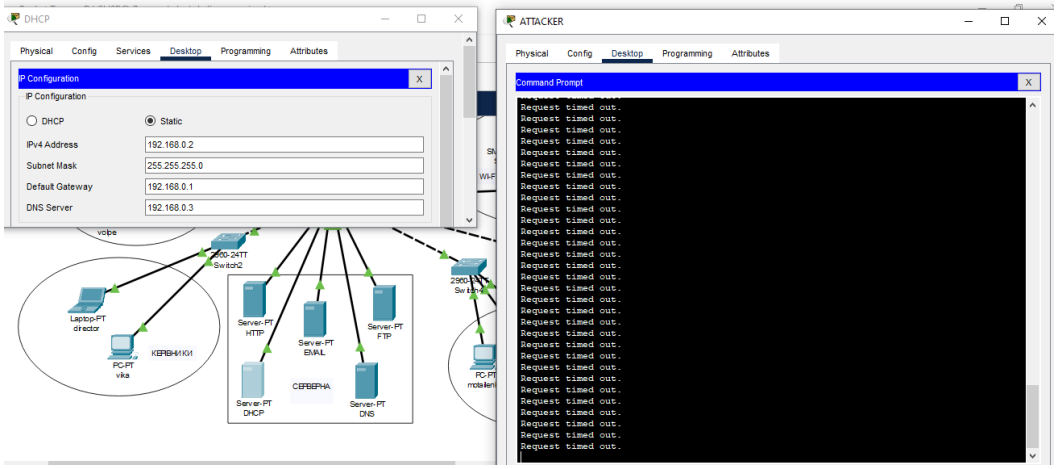

Рисунок 3.15 – Проведено атаку на сервер. VLAN успішно запобіг атаці

Сценарій №2

У цьому сценарії зловмисник, видаючи себе за клієнта компанії, підключається до Wi–Fi у зоні для відвідувачів. Після отримання доступу до мережі він починає здійснювати DoS–атаку, спрямовану на внутрішні сервери компанії. Атака проходить через міжмережевий екран (firewall), який стоїть між гостьовою мережею та внутрішньою інфраструктурою.

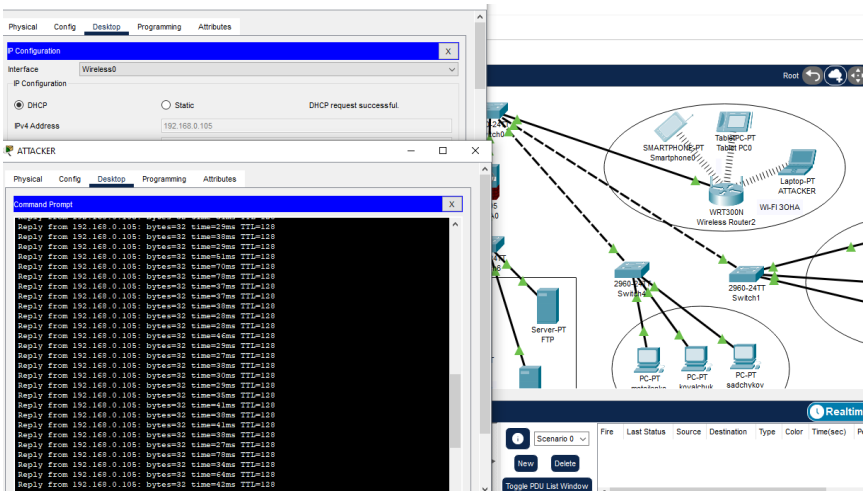

Рисунок 3.16 – Було здійснено DoS–атаку на гостьовий планшет. З точки зору зловмисника, атака виявилася успішною

На рисунку 3.17 продемонстровано ефективність роботи міжмережевого екрану (firewall), який успішно заблокував спробу атаки, що забезпечило захист мережі від потенційних загроз і запобігло порушенню її нормального функціонування. Цей результат підтверджує важливість впровадження засобів мережевого захисту для підтримки безпеки корпоративної інфраструктури.

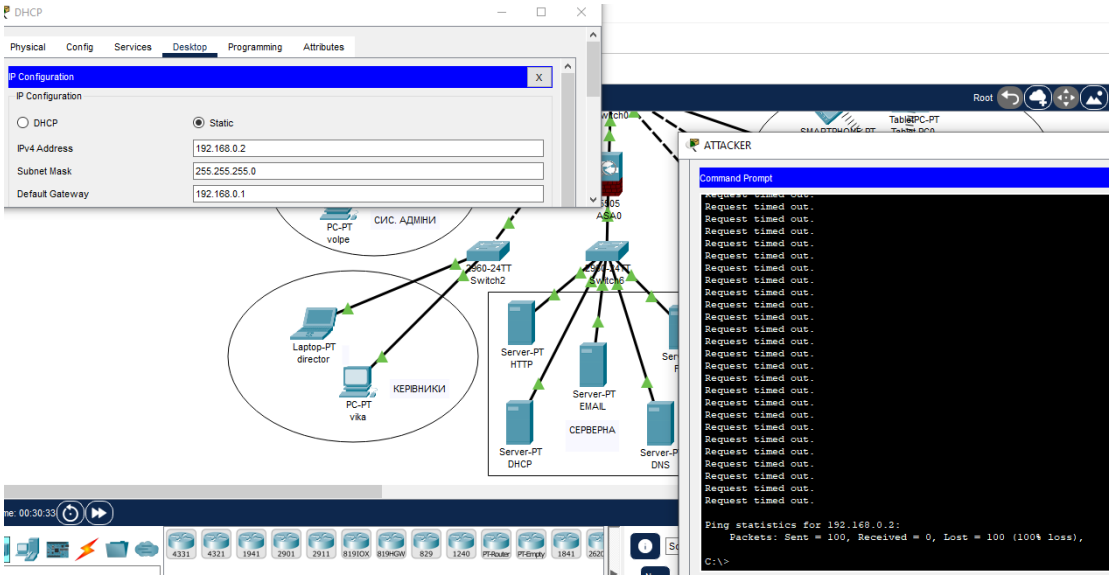

Рисунок 3.17 – Firewall успішно запобіг атаці

Сценарій № 3

У цьому сценарії зловмисник, який є внутрішнім працівником компанії, перебуває у філії (другому офісі) та має доступ до корпоративної мережі через VPN–з'єднання. Використовуючи свій доступ, він ініціює DoS–атаку, спрямовану на головний сервер компанії, намагаючись перевантажити його та порушити стабільну роботу сервісів. Атака здійснюється зсередини мережі через захищений канал, що ускладнює її виявлення традиційними засобами моніторингу. Сценарій моделює ситуацію, коли загроза походить від легітимного користувача з повним доступом до внутрішніх ресурсів. На Рис. 3.18 зображено атаку на DHCP-сервер, здійснену з іншого офісу.

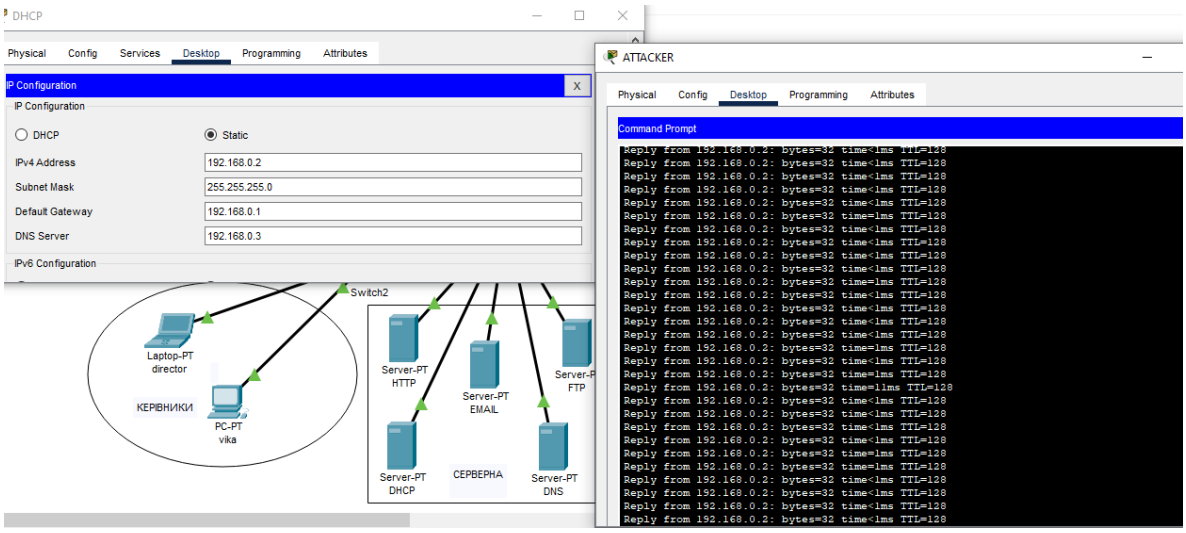

Рисунок 3.18 Атака на DHCP сервер

Висновок:

У результаті моделювання було розглянуто три різні сценарії розвитку подій при DoS–атаках у локальній мережі, кожен з яких продемонстрував ефективність або вразливість певного механізму захисту.

У першому сценарії була реалізована сегментація за допомогою VLAN. Атака на звичайний пристрій (планшет) в межах того самого VLAN виявилася успішною, оскільки між зловмисником і жертвою не було встановлено жодних бар'єрів. Натомість атака на критичний сервіс – DHCP–сервер – з іншого VLAN була заблокована, що засвідчило ефективність ізоляції трафіку між логічно розділеними сегментами мережі.

У другому сценарії захист було реалізовано через міжмережевий екран (firewall) із налаштованими рівнями безпеки. У цьому випадку спроба атаки на DHCP–сервер з менш довіреного сегмента мережі була успішно заблокована, що підтвердило ефективність фільтрації трафіку за правилами доступу та принципом зони довіри.

У третьому сценарії до інфраструктури було додано VPN–тунель для забезпечення захищеного з’єднання між вузлами. Шифрування трафіку дозволило захистити передані дані від перехоплення, однак DoS–атака на сервер в межах встановленого тунелю все ж була успішною. Це підкреслює, що VPN не є засобом захисту від атак типу відмови в обслуговуванні, адже його завдання –

гарантувати конфіденційність та цілісність трафіку, а не фільтрацію чи обмеження доступу.

Таким чином, результати моделювання підтвердили: жоден із засобів захисту не є універсальним. Найкращі результати досягаються шляхом поєднання кількох механізмів – сегментації мережі, контролю доступу, міжмережевого екранування та шифрування трафіку – що дозволяє забезпечити як ізоляцію, так і захист даних на різних рівнях взаємодії в мережі.

3.3 Аналіз ефективності різних механізмів захисту

У ході моделювання було перевірено ефективність двох популярних засобів захисту мережі – VLAN та Firewall – проти атак типу DoS і MAC Flooding.

VLAN забезпечує логічне сегментування мережі, ізолюючи трафік між різними групами користувачів. Це дозволяє обмежити зону поширення атаки в межах одного сегменту. Зокрема, було продемонстровано, що DoS–атака, ініційована з однієї VLAN, не змогла досягти серверів, які знаходяться в іншій VLAN. Це доводить ефективність VLAN у контексті стримування загроз між сегментами. Однак, якщо зловмисник знаходиться в тій самій VLAN, атака проходить успішно, оскільки VLAN не контролює трафік всередині сегменту і не виявляє складні атаки. Крім того, неправильне налаштування VLAN може призвести до витоку трафіку або порушень безпеки.

Firewall (міжмережевий екран) надає більш гнучкий і глибокий контроль над трафіком, дозволяючи обмежити доступ не лише за логічним сегментуванням, а й на основі політик безпеки, портів, IP–адрес, та рівнів довіри. У змодельованому сценарії firewall успішно заблокував DoS–атаку на критичний сервер, попри те, що атакуючий перебував у підключеній до мережі зоні. Це демонструє, що firewall забезпечує більш детальний рівень контролю, особливо для захисту ключових ресурсів. Проте, firewall вимагає ретельного налаштування та регулярного оновлення правил, а помилки в конфігурації можуть призводити до пропуску атак або блокування легітимного трафіку.

Також firewall не завжди ефективний проти складних чи цілеспрямованих атак, які можуть обходити прості правила.

Для підвищення рівня безпеки мережі часто використовують додаткові засоби, такі як системи виявлення та запобігання вторгненням (IDS/IPS). Вони виконують глибокий аналіз мережевого трафіку в реальному часі, виявляючи аномалії та потенційні загрози, наприклад, спроби сканування портів, підробку пакетів чи надмірне навантаження, яке може сигналізувати про атаку. IDS/IPS можуть автоматично блокувати підозрілі дії, однак їх ефективність значною мірою залежить від правильного налаштування і регулярного оновлення баз сигнатур, інакше можливі численні хибні спрацювання.

Хмарні firewall, такі як рішення від провайдерів типу AWS, Azure або Cloudflare, забезпечують розподілений захист від великих DDoS–атак, розподіляючи трафік через глобальні дата–центри і фільтруючи шкідливі пакети до того, як вони досягнуть локальної мережі. Такий підхід особливо корисний для компаній із великою кількістю віддалених офісів або веб–сервісів, але при цьому користувачі залежать від стабільності інтернет–з'єднання, а також існують ризики, пов'язані з довірою до стороннього провайдера, який має доступ до трафіку.

VPN (віртуальна приватна мережа) забезпечує шифроване з'єднання для безпечного доступу віддалених співробітників до корпоративної мережі, захищаючи дані від перехоплення в незахищених мережах. Проте VPN сам по собі не перешкоджає атакам всередині мережі або поширенню загроз між сегментами, тому його використання слід поєднувати з іншими засобами безпеки. Також VPN може знижувати швидкість інтернет–з'єднання через додаткове шифрування і маршрутизацію.

Таким чином, кожен з цих механізмів має свої специфічні переваги й обмеження, і їхнє комбіноване застосування забезпечує більш комплексний і надійний захист мережі.

3.4 Практичні рекомендації щодо покращення безпеки локальних мереж

Практичні рекомендації щодо покращення безпеки локальних мереж мають охоплювати широкий спектр заходів, які допомагають захистити інфраструктуру від різноманітних загроз. Слід впроваджувати багаторівневий захист – це означає не покладатися лише на один метод, а поєднувати сегментацію мережі, міжмережеві екрани, системи виявлення вторгнень, а також шифрування даних. Дуже важливо регулярно оновлювати всі мережеві пристрої та програмне забезпечення, щоб закривати відомі вразливості й уникати атак через експлойти.

Аутентифікація користувачів має бути максимально суворою – використання багатофакторної аутентифікації (MFA) значно знижує ризик несанкціонованого доступу. Керування доступом має будуватися за принципом найменших привілеїв, коли кожен користувач або пристрій має доступ лише до тих ресурсів, які потрібні для виконання їхніх завдань. Впровадження VPN з надійним шифруванням забезпечить безпечне підключення віддалених користувачів, а мережеві політики та правила firewall допоможуть контролювати і обмежувати трафік.

Також варто застосовувати регулярний моніторинг мережі з використанням систем логування та аналізу подій безпеки. Це дозволяє своєчасно виявляти підозрілі дії і реагувати на них до того, як вони призведуть до серйозних наслідків. Резервне копіювання даних має бути обов’язковою практикою, а перевірка можливості відновлення інформації – регулярною процедурою.

Не менш важливою є підготовка персоналу – навчання співробітників основам кібергігієни, розпізнаванню фішингових атак і правильному поводженню з паролями допомагає знизити людський фактор у загрозах. Впровадження фізичного захисту обладнання – обмеження доступу до серверних

кімнат, використання камер відеоспостереження та систем контролю доступу – додає ще один рівень безпеки.

Загалом, комплексний підхід, що включає технічні, організаційні та людські аспекти, є ключем до забезпечення надійного захисту локальних мереж від сучасних кіберзагроз.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було проведено ґрунтовне теоретичне й практичне дослідження проблем інформаційної безпеки локальних комп'ютерних мереж. Встановлено, що з розвитком цифрових технологій локальні мережі стають не лише критично важливими елементами IT–інфраструктури, а й дедалі вразливішими до широкого спектра загроз – як внутрішніх, так і зовнішніх. Сучасні умови вимагають не просто впровадження окремих засобів захисту, а формування комплексного, багаторівневого підходу до кібербезпеки, що охоплює як технічні рішення, так і організаційні заходи.

У роботі класифіковано основні типи загроз, серед яких внутрішні, такі як несанкціонований доступ, витік конфіденційної інформації, помилки адміністрування та внутрішні шкідливі програми, а також зовнішні – мережеві атаки, фішинг, DDoS, SQL–ін'єкції, експлойти та інші. Особливу увагу приділено аналізу вразливостей інфраструктури та людського чинника, який часто є джерелом найнебезпечніших інцидентів.

Практична частина дослідження включала моделювання реальних атак у середовищі Cisco Packet Tracer. Було перевірено ефективність таких засобів захисту, як VLAN, міжмережеві екрани (firewall) та VPN–тунелі. Проведено три сценарії DoS–атак з різних векторів доступу: з гостьового сегменту, між VLAN та через VPN. Результати засвідчили, що жоден окремий механізм не забезпечує абсолютного захисту, однак їхнє поєднання суттєво підвищує загальну стійкість мережі до загроз.

У процесі моделювання підтверджено ефективність використання систем виявлення та запобігання вторгнень для виявлення аномального трафіку, систем централізованого моніторингу та аудиту подій, технологій шифрування для забезпечення конфіденційності даних, механізмів контролю доступу для обмеження прав користувачів, а також хмарних рішень, що забезпечують масштабований та розподілений захист мереж.

На основі проведеного аналізу сформульовано комплекс практичних рекомендацій, серед яких впровадження багатофакторної автентифікації, регулярне оновлення програмного забезпечення та баз сигнатур, резервне копіювання даних, навчання персоналу правилам кібергігієни та посилення фізичного контролю доступу до критичних компонентів інфраструктури.

Таким чином, результати кваліфікаційної роботи підтверджують необхідність реалізації комплексної системи безпеки, яка повинна охоплювати не лише технічні засоби, а й організаційні політики, стандарти управління доступом, системи реагування на інциденти та постійне підвищення обізнаності персоналу. Запропоновані підходи є універсальними й можуть бути ефективно впроваджені у малих, середніх та великих організаціях для забезпечення надійного рівня захисту локальних мереж в умовах постійного зростання кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Таненбаум А. С., Уэзеролл Д. Дж. Комп’ютерні мережі. – 5–те видання. – СПб.: Пітер, 2013. – 960 с.

2. Kurose J. F., Ross K. W. Computer Networking: A Top–Down Approach. – 8th ed. – Pearson, 2020. – 864 p.

3. Чабаненко С. А. Інформаційна безпека комп’ютерних мереж. – К.: Ліра–К, 2016. – 248 с.

4. Романовський В. І. Засоби захисту інформації в комп’ютерних системах. – Харків: ХНУРЕ, 2018. – 312 с.

5. Cisco Networking Academy: Learn Cybersecurity, Python & More. Cisco Networking Academy: Learn Cybersecurity, Python & More. URL: https://www.netacad.com/ (date of access: 12.04.2025).

6. Житомирський В. М. Безпека комп’ютерних систем і мереж. – К.: ВНТУ, 2020. – 198 с.

7. Андрущенко Т. А. Комп’ютерна безпека: методи, засоби та політика захисту. – К.: Наукова думка, 2021. – 220 с.

8. NIST Special Publication 800–41 Rev.1. Guidelines on Firewalls and Firewall Policy. – National Institute of Standards and Technology, 2009.

9. Марчук В. В. Кібербезпека: навчальний посібник. – К.: Академвидав, 2021. – 260 с.

10. Столл К. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. – New York: Pocket Books, 2005.

11. Слободянюк О. М. Архітектура комп’ютерних мереж та інформаційна безпека. – Тернопіль: ТНТУ, 2020. – 212 с.

12. Бровченко В. Г. Адміністрування комп’ютерних мереж. – К.: Основа, 2017. – 180 с.

13. Журавльов О. П. Теорія і практика побудови захищених комп’ютерних систем. – Харків: ХНУРЕ, 2019. – 296 с.

14. Учасники проектів Вікімедіа. VPN – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/VPN (дата звернення: 10.04.2025).

15. Учасники проектів Вікімедіа. Система запобігання вторгнень – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_запобігання_вторгнень (дата звернення: 08.06.2025).

16. Учасники проектів Вікімедіа. Система запобігання вторгнень – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Система_запобігання_вторгнень (дата звернення: 08.04.2025).

17. Учасники проектів Вікімедіа. Локальна мережа – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Локальна_мережа (дата звернення: 02.04.2025).

18. Учасники проектів Вікімедіа. Локальна мережа – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Локальна_мережа (дата звернення: 23.03.2025).

19. Гребенюк В. А., Красюк В. В. Інформаційна безпека: теорія та практика. – Харків: ХНУРЕ, 2020. – 280 с.

20. Романенко В. В. Комп’ютерна безпека: навчальний посібник. – Львів: Видавництво ЛНУ, 2021. – 224 с.

21. Stallings W. Network Security Essentials: Applications and Standards (6th Edition). – Pearson, 2020. – 496 p.

22. Лозинський О. Л. Основи кібербезпеки. – Чернівці: ЧНУ, 2022. – 198 с.