Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: "Технології та методи захисту корпоративних мереж"

Виконав: студент (ка) IV курсу, групи СБ-41

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Добруцький Олександр Романович
підпис (прізвище та ініціали)

Керівник Лечаченко Т. А.
підпис (прізвище та ініціали)

Нормоконтроль Дроздова Т.В.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Стоянов Ю.М.
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Добруцькому Олександру Романовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Технології та методи захисту корпоративних мереж

Керівник роботи Лечаченко Тарас Анатолійович, PhD доктор філософії., старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «__» ___ 2025 року № _____

2. Термін подання студентом завершеної роботи 14.06.2025

3. Вихідні дані до роботи Системні вимоги для роботи з даним ПЗ включають операційну систему Microsoft Windows 10/11 (64-bit), процесор Intel Core i3, 4 ГБ оперативної пам'яті та 1 ГБ вільного дискового простору, прикладне програмне забезпечення Cisco Packet Tracer 8.2

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати сучасні загрози та вразливості корпоративних мереж, а також актуальні підходи до їх захисту.
Розробити архітектуру та модель безпеки корпоративної мережі з використанням міжмережевого екрану.
Здійснити практичну реалізацію розробленої архітектури в програмному середовищі Packet Tracer та налаштування ключових компонентів захисту.
Провести тестування та оцінку ефективності впроваджених заходів захисту.
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Топологія та методи захисту корпоративних мереж. Актуальність теми: Зростання кіберзагроз. Мета та завдання роботи. Загальні сучасні кіберзагрози. Аналіз потенційних загроз та вразливостей. Розроблена топологія корпоративної мережі. Модель безпеки та принципи захисту. Практична реалізація: Налаштування обладнання. Оцінка ефективності захисту: Успішні тести. Оцінка ефективності захисту: Блокування. Висновки. Перспективи подальших досліджень.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С.Ю., проф. кафедри МТ		

7. Дата видачі завдання 29.01.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	20.01 – 23.01	Виконано
2.	Підбір та опрацювання джерел для аналізу сучасних загроз та вразливостей корпоративних мереж	25.01 – 05.02	Виконано
3.	Аналіз існуючих підходів та технологій захисту корпоративних мереж	06.02 – 20.02	Виконано
4.	Розроблення архітектури та моделі безпеки корпоративної мережі з використанням міжмережевого екрану Cisco ASA Firewall	22.02 – 12.03	Виконано
5.	Практична реалізація розробленої архітектури в програмному середовищі Cisco Packet Tracer	15.03-25.03	Виконано
6.	Детальне налаштування ключових компонентів захисту (маршрутизації, зон безпеки, правил контролю доступу) на Cisco ASA Firewall та інших пристроях	25.02 – 10.04	Виконано
7.	Проведення тестування та оцінки ефективності впроваджених заходів захисту корпоративної мережі	10.02 – 05.03	Виконано
8.	Оформлення розділу "Дослідження актуальних загроз та вимог до систем захисту корпоративних мереж"	26.03 – 04.05	Виконано
9.	Оформлення розділу "Опис топології корпоративної мережі та її моделі безпеки".	12.04-20.04	Виконано
10.	Оформлення розділу "Практична реалізація та оцінка ефективності заходів захисту корпоративної мережі".	25.04 – 10.05	Виконано
11.	Виконання завдання до підрозділу "Безпека життєдіяльності та основи охорони праці".	06.05 – 14.05	Виконано
12.	Оформлення кваліфікаційної роботи	23.05 – 08.06	Виконано
13.	Нормоконтроль	10.06 – 15.06	Виконано
14.	Перевірка на плагіат	20.06 – 22.06	Виконано
15.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	Виконано
16.	Захист кваліфікаційної роботи	25.06.2025	

Студент _____ Добруцький О.Р.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Лечаченко Т. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Технології та методи захисту корпоративних мереж // Кваліфікаційна робота ОР «Бакалавр» // Добруцький Олександр Романович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2025 // С. 63 рис. – 7, табл. – 0, кресл. – 0, додат. – 0.

Ключові слова: корпоративна мережа, кібербезпека, Cisco ASA, Packet Tracer, міжмережевий екран.

Дана кваліфікаційна робота присвячена розробці і впровадженню комплексу заходів для забезпечення надійного захисту корпоративної мережі від сучасних кіберзагроз. У роботі проведено аналіз актуальних вразливостей та атак, що становлять небезпеку для інформаційних систем, а також розглянуто основні підходи до їх протидії. Розроблено архітектуру захищеної корпоративної мережі з використанням міжмережевого екрану Cisco ASA Firewall, яка включає центральний офіс, філію та демілітаризовану зону. Здійснено практичну реалізацію цієї архітектури в програмному середовищі Cisco Packet Tracer, включаючи детальне налаштування маршрутизації, зон безпеки та правил контролю доступу. Проведено тестування впроваджених рішень для оцінки їх ефективності в умовах імітації реальних загроз. Окрему увагу приділено питанням охорони праці та гігієнічним вимогам до умов роботи з відеодисплейними терміналами, а також принципам цивільного захисту в контексті функціонування інформаційної інфраструктури. Результати роботи підтверджують високу ефективність запропонованих заходів для підвищення рівня інформаційної безпеки корпоративної мережі.

ABSTRACT

Technologies and methods for protecting corporate networks // Qualification Paper for Bachelor's Degree // Dobrutskyi Oleksandr // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, Group SB-41 // Ternopil, 2025 // P. 62, Fig. – 7, Tab. – 0, Drawings – 0, Appendices – 0.

Keywords: corporate network, cybersecurity, Cisco ASA, Packet Tracer, firewall.

This qualification paper is dedicated to the development and implementation of a set of measures to ensure reliable protection of a corporate network against modern cyber threats. The paper analyzes current vulnerabilities and attacks that pose a danger to information systems, and examines the main approaches to counteracting them. An architecture for a secure corporate network utilizing the Cisco ASA Firewall was developed, which includes a central office, a branch office, and a demilitarized zone. The practical implementation of this architecture was carried out in the Cisco Packet Tracer software environment, including detailed configuration of routing, security zones, and access control rules. Testing of the implemented solutions was conducted to evaluate their effectiveness under simulated real threats. Special attention was paid to occupational safety issues and hygienic requirements for working conditions with visual display terminals, as well as the principles of civil protection in the context of information infrastructure functioning. The results of the work confirm the high effectiveness of the proposed measures in increasing the level of information security of the corporate network.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ASA	—	Adaptive Security Applience
ACL	—	Access Control List
DMZ	—	Demilitarized Zone
DoS	—	Denial of Service
DDoS	—	Distributed Denial of Service
IDS	—	Intrusion Detection System
IPS	—	Intrusion prevention System
NAT	—	Network Address Translation
ВДТ	—	Відеодисплейний термінал
ЗІЗ	—	Засоби індивідуального захисту
НС	—	Надзвичайна ситуація
дБ	—	Децибел
лк	—	Люкс
К	—	Кельвін

ВСТУП

Сучасний світ характеризується стрімким розвитком інформаційних технологій, що стали фундаментом для функціонування абсолютної більшості організацій, незалежно від їхнього масштабу та сфери діяльності. Корпоративні мережі є критично важливим активом, що забезпечує зберігання, обробку та передачу конфіденційних даних, підтримку ключових бізнес-процесів та комунікацію між співробітниками, партнерами та клієнтами. Ця всеосяжна цифровізація призводить до значної залежності від безперебійного та безпечного функціонування інформаційної інфраструктури.

Однак, паралельно з розвитком технологій, спостерігається і безпрецедентне зростання кількості та складності кіберзагроз. Сучасний кіберпростір став ареною для постійної протидії між зловмисниками (кіберзлочинцями, хактивістами, державними суб'єктами) та фахівцями з кібербезпеки. Атаки стають більш цілеспрямованими, витонченими та диверсифікованими, використовуючи нові вектори зараження та експлуатуючи як технічні вразливості, так і людський фактор. Це включає широкий спектр загроз, від шкідливого програмного забезпечення нового покоління (наприклад, складні програми-вимагачі, здатні шифрувати не тільки файли, а й цілі файлові системи) та цілеспрямованих атак (Advanced Persistent Threats – APT), до складних фішингових кампаній та масових DDoS-атак, що можуть повністю паралізувати діяльність організації.

Наслідки успішних кібератак виходять далеко за межі простих фінансових втрат. Вони можуть включати компрометацію конфіденційної інформації (витік персональних даних, комерційної таємниці), зупинку бізнес-процесів через простої систем, а також значні репутаційні збитки, що підривають довіру клієнтів та партнерів. Крім того, недотримання стандартів безпеки може стати причиною юридичних позовів та штрафів. В умовах, коли корпоративні мережі стають все більш складними, розподіленими (з використанням хмарних сервісів, віддалених робочих місць), а кіберзагрози постійно мутують, виникає нагальна потреба у розробці та впровадженні ефективних, адаптивних та

багаторівневих систем захисту. Тому дослідження та розробка підходів до комплексного захисту корпоративних мереж є надзвичайно актуальним завданням для забезпечення стійкості, безперервності функціонування та розвитку будь-якої організації у цифрову епоху.

Метою кваліфікаційної роботи є розробка і обґрунтування комплексу технологій та методів, спрямованих на підвищення рівня захищеності корпоративних мереж від сучасних кіберзагроз, з особливим акцентом на практичні аспекти їх реалізації та тестування.

Для досягнення поставленої мети були сформульовані наступні задачі дослідження: провести аналіз актуальних загроз та викликів у сфері захисту корпоративних мереж, а також визначити ключові вимоги до систем безпеки; розробити узагальнену архітектуру системи захисту корпоративної мережі, визначити основні компоненти та принципи їх взаємодії; обґрунтувати вибір конкретних політик безпеки та засобів захисту, які відповідатимуть визначеним вимогам та моделям; реалізувати (або змоделювати) проектні рішення з захисту корпоративної мережі, застосовуючи обрані технології та методи; провести тестування розробленої (або змодельованої) системи захисту для оцінки її ефективності та виявлення можливих недоліків; розглянути питання безпеки життєдіяльності та основ охорони праці, що є релевантними для фахівців, які працюють з інформаційними системами та мережевим обладнанням.

Об'єктом дослідження є процес забезпечення інформаційної безпеки корпоративних мереж. Це охоплює взаємодію між мережевим обладнанням, програмним забезпеченням, даними та користувачами в умовах постійного впливу зовнішніх та внутрішніх загроз, а також методи та принципи, що застосовуються для протидії цим загрозам.

Предметом дослідження є технології та методи побудови багаторівневої системи захисту корпоративних мереж, що дозволяють забезпечити конфіденційність, цілісність та доступність інформаційних ресурсів. Це включає аналіз і практичне застосування мережевої сегментації, міжмережевих екранів, систем контролю доступу, а також методологій тестування ефективності захисту.

Одержані в результаті виконання кваліфікаційної роботи результати мають значне практичне значення. Вони надають обґрунтовану методологію для аналізу потреб та проектування систем захисту корпоративних мереж, що може бути використана IT-спеціалістами та фахівцями з кібербезпеки на підприємствах. Крім того, робота демонструє практичні аспекти реалізації ключових захисних механізмів, таких як мережева сегментація, налаштування міжмережевих екранів та управління доступом, на прикладі змодельованої мережі, а описані конфігурації можуть слугувати основою для впровадження подібних рішень у реальних умовах. Важливо, що робота підкреслює необхідність тестування систем безпеки для виявлення вразливостей та оцінки ефективності захисту, сприяючи підвищенню загального рівня кіберстійкості організацій. Отримані результати також сприяють підвищенню обізнаності щодо сучасних кіберзагроз та методів протидії, що є критично важливим для формування компетентних кадрів у сфері кібербезпеки. Нарешті, матеріали роботи можуть бути використані як навчальний матеріал для студентів та фахівців, що вивчають або підвищують кваліфікацію в галузі захисту інформації в комп'ютерних системах і мережах.

Таким чином, результати роботи є актуальними для широкого кола організацій, що прагнуть забезпечити надійний захист своїх інформаційних активів в умовах зростаючих кіберзагроз.

РОЗДІЛ 1 ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ЗАГРОЗ ТА ВИМОГ ДО СИСТЕМ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Актуальність проблеми захисту корпоративних мереж

В сучасному світі, де цифровізація стала невід'ємною частиною функціонування будь-якого підприємства, корпоративні мережі перетворилися на центральний нервовий вузол бізнесу. Вони є системою, що забезпечує зберігання, обробку та передачу життєво важливої інформації, підтримуючи всі бізнес-процеси та комунікації. Безперебійна та безпечна робота цієї інфраструктури є критично важливою для виживання та розвитку компанії. Однак, паралельно з цією тотальною інтеграцією, зростає і кількість, і складність кіберзагроз, перетворюючи кіберпростір на поле постійної боротьби. Атаки стають все більш цілеспрямованими та витонченими, експлуатуючи не тільки технічні вразливості, а й людський фактор. Це створює нагальну проблему захисту корпоративних мереж, яка вимагає глибокого розуміння природи загроз та розробки комплексних методів протидії [1, 6].

Можливі загрози для корпоративних мереж є різноманітними та постійно еволюціонують. Однією з найбільш поширених та підступних загроз є аналіз мережевого трафіку. Цей метод є надзвичайно ефективним для отримання несанкціонованого доступу до конфіденційної інформації, такої як логіни та паролі користувачів. Зловмисники використовують спеціалізовані програми – аналізатори пакетів (packet sniffers), які перехоплюють весь мережевий трафік, що проходить через певний сегмент мережі. Після перехоплення, ці програми аналізують вміст пакетів, виділяючи ті, що містять ідентифікаційні дані та паролі користувачів. Проблема полягає в тому, що у багатьох застарілих або неправильно налаштованих протоколах, таких як SMTP (для електронної пошти), HTTP (для веб-сторінок без шифрування), FTP (для передачі файлів), POP3, TELNET, IMAP, IRC та NNTP, дані передаються у відкритому, незашифрованому вигляді. Це робить їх надзвичайно вразливими для перехоплення та розшифрування. Успішний аналіз мережевого трафіку може

призвести до блокування доступу до поштових систем, крадіжки номерів кредитних карток, розголошення конфіденційної інформації, що передається між співробітниками, та інших особистих даних. Хоча існують сучасні протоколи, які забезпечують захист мережевих з'єднань та шифрування трафіку (наприклад, HTTPS, SFTP, SMTPS), їхнє повсюдне впровадження досі залишається проблемою. Історично, обмеження на експорт криптографічних інструментів у деяких країнах призвели до того, що реалізації цих протоколів не були повсюдно вбудовані в програмне забезпечення або мали обмежену ефективність. Це залишає значні "вікна вразливості" у багатьох корпоративних мережах.

Крім того, аналіз мережевого трафіку може бути використаний не лише для крадіжки даних, але й для вивчення логіки роботи розподіленої комп'ютерної системи. Перехоплюючи потоки даних, що обмінюються об'єкти в такій системі, зловмисник може встановити однозначну відповідність між певними подіями та командами, що відбуваються в системі. Це дозволяє створювати детальні профілі роботи системи та її компонентів, що надалі може бути використано для симуляції та виконання віддалених атак на практиці. Наприклад, знаючи послідовність команд для доступу до певного сервісу, зловмисник може відтворити цю послідовність, обходячи при цьому базові механізми захисту. Слід зауважити, що аналіз трафіку в його пасивній формі можливий лише в межах одного сегмента мережі, де зловмисник може перехоплювати пакети (наприклад, через ARP-spoofing або підключення до неконтрольованого порту комутатора [2]), і він не надає можливості змінювати сам трафік. Однак, навіть пасивне перехоплення є надзвичайно небезпечним через потенційні наслідки для конфіденційності та цілісності інформаційної безпеки в скомпрометованому сегменті мережі.

Ще однією критичною проблемою безпеки розподіленої комп'ютерної мережі є неадекватна ідентифікація та автентифікація віддалених об'єктів. У ситуаціях, коли об'єкти системи (сервери, клієнти, додатки) взаємодіють між собою через мережу, виникає нагальна потреба в їхній однозначній ідентифікації та підтвердженні їхньої справжності. Для вирішення цієї

проблеми у розподілених системах часто застосовують механізми створення віртуальних каналів з подальшим обміном інформацією для ідентифікації, що іноді називається "рукостисканням" (handshake). Однак, цей метод не завжди застосовується для всіх віддалених об'єктів або може бути реалізований з недоліками, що створює вразливості. Наприклад, для ідентифікації об'єктів розподіленої системи традиційно використовують мережеві адреси (IP-адреси), які мають бути унікальними для кожного об'єкта. Проте, варто враховувати, що ці адреси можуть бути піддаватися підробці (IP-spoofing), коли зловмисник видає себе за інший легітимний об'єкт, використовуючи його IP-адресу. Це ускладнює їх використання як однозначного та надійного ідентифікатора об'єктів та відкриває двері для атак "людина посередині" або несанкціонованого доступу.

Окрім зазначених загроз, існують також інші, не менш небезпечні:

- Шкідливе програмне забезпечення (малваре), що еволюціонує: Це включає програми-вимагачі (ransomware), які шифрують дані та вимагають викуп, віруси, троянські програми, шпигунське ПЗ та руткіти. Вони здатні обійти традиційні засоби захисту, швидко поширюватися по мережі та наносити колосальні фінансові та репутаційні збитки, паралізуючи роботу організації [6, 10].
- Фішинг та соціальна інженерія: Ці атаки використовують психологічні маніпуляції, щоб примусити користувачів розкрити конфіденційну інформацію або виконати шкідливі дії. Вони є надзвичайно ефективними, оскільки спрямовані на "людську вразливість" [6] і можуть обійти найсучасніші технічні засоби захисту.
- Вразливості програмного забезпечення та обладнання: Недоліки у коді або конфігурації операційних систем, мережевого обладнання та додатків створюють "вікна" для зловмисників. Несвоєчасне оновлення або ігнорування патчів безпеки дозволяє хакерам експлуатувати ці вразливості [17], отримуючи несанкціонований доступ.

Всі ці загрози створюють надзвичайно складний та динамічний ландшафт кібербезпеки. Для їх ефективної нейтралізації потрібен не просто набір окремих

інструментів, а комплексна, багаторівнева система захисту, що постійно адаптується до нових викликів. Саме тому питання розробки та впровадження сучасних технологій та методів захисту корпоративних мереж є не просто актуальним, а критично важливим завданням для забезпечення безперервності та стійкості функціонування будь-якої організації у цифровому світі.

1.2 Вимоги до системи захисту інформації в корпоративній мережі

Побудова ефективної системи захисту інформації (СЗІ) в корпоративній мережі вимагає чіткого визначення вимог, які формуються на основі бізнес-процесів, інформаційних активів, кіберзагроз та регуляторних зобов'язань [4, 20]. Сформульовані вимоги слугують дорожньою картою для проектування та оцінки ефективності СЗІ.

Розглядаючи функціональні вимоги до СЗІ, вони охоплюють ключові аспекти контролю та захисту. По-перше, глибокий контроль мережевого трафіку є ключовим. Сучасна СЗІ повинна виконувати глибоку інспекцію пакетів (DPI) для аналізу та блокування прихованих загроз [3, 14]. Це доповнюється безперервним моніторингом трафіку в реальному часі, що є критично важливим для оперативного виявлення аномалій та кібератак.

По-друге, мережева сегментація та зонування безпеки є необхідними елементами. Це передбачає логічне або фізичне розділення мережі на ізольовані сегменти (VLAN) для ускладнення горизонтального поширення загрози. Окрім того, обов'язковим є створення демілітаризованих зон (DMZ) як буферних зон між Інтернетом та внутрішньою мережею для розміщення загальнодоступних сервісів [2, 7].

Надійне управління ідентифікацією та доступом забезпечує конфіденційність і цілісність інформації, надаючи доступ лише авторизованим користувачам. Центральними елементами цього є реалізація багатофакторної аутентифікації (MFA) та використання систем управління ідентифікацією та доступом (IAM) [11, 12]. Додатково для гранульованого контролю застосовуються списки контролю доступу (ACL).

Серед інших функціональних вимог – інтеграція передових систем виявлення та запобігання вторгненням (IDS/IPS). Ці механізми виявляють та активно перешкоджають атакам, причому IDS пасивно моніторять трафік, генеруючи сповіщення, а IPS здатні автоматично блокувати шкідливий трафік у реальному часі [6, 11].

Комплексний, багаторівневий захист від шкідливого програмного забезпечення вимагає стратегії "глибокої оборони", що включає захист на кінцевих точках (антивірус, EDR), на мережевому периметрі (фільтрація шкідливого ПЗ на шлюзах) та використання "пісочниць" (Sandboxing) для виявлення нових загроз [10, 18].

Безпечний віддалений доступ та використання віртуальних приватних мереж (VPN) передбачає створення зашифрованих тунелів через загальнодоступну мережу. Це забезпечує безпечне підключення віддалених користувачів та філіалів до корпоративних ресурсів, гарантуючи конфіденційність, цілісність та автентифікацію трафіку [14].

Нарешті, централізоване та детальне журналювання з можливістю аудиту подій безпеки є основою для моніторингу, виявлення інцидентів та розслідувань. Воно включає детальне журналювання подій на всіх рівнях інфраструктури, централізоване зберігання та кореляцію журналів за допомогою SIEM-систем [13].

Нефункціональні вимоги до СЗІ визначають якість та ефективність її функціонування. Першою з них є висока продуктивність та масштабованість. СЗІ не повинна створювати затримок у мережі та має бути здатною легко збільшувати потужності у відповідь на зростання обсягу даних та користувачів.

Далі, надійність, відмовостійкість та відновлюваність є важливими для безперебійної роботи, функціонування у випадку відмови компонентів (завдяки надлишковості, кластеризації, механізмам Failover) та швидкого повернення до повного функціонального стану після збоїв (за допомогою DRP) [4].

Керованість, зручність експлуатації та інтеграція передбачають наявність централізованої консолі управління для спрощення адміністрування,

автоматизацію рутинних завдань та безшовну інтеграцію з IAM, моніторингом та SIEM-системами.

Безпека самої системи захисту є невід'ємною вимогою: компоненти СЗІ повинні бути захищені від несанкціонованого доступу та модифікації. Це досягається завдяки регулярним оновленням, жорстким політикам доступу, MFA для адміністрування та мінімізації поверхні атаки.

І, нарешті, відповідність нормативно-правовим актам та стандартам є обов'язковою. СЗІ повинна відповідати вимогам чинного законодавства, внутрішнім політикам компанії та галузевим стандартам (ISO/IEC 27001, NIST, PCI DSS) [4, 20].

1.3 Аналіз архітектурних рішень та технологій захисту корпоративних мереж

Сучасні корпоративні мережі стикаються зі зростаючим рівнем кіберзагроз, що вимагає застосування комплексних, багаторівневих підходів до захисту. Ефективна система захисту інформації (СЗІ) – це екосистема взаємопов'язаних технологій, політик та процедур. Аналіз існуючих архітектурних рішень та технологій є критично важливим для реалізації вимог СЗІ, а вибір залежить від специфічних потреб організації.

Одним з фундаментальних принципів СЗІ є "глибока оборона" (defense in depth) [1]. Цей принцип передбачає розгортання кількох рівнів захисту (фізичний, мережевий периметр, внутрішня мережева сегментація, захист кінцевих точок, додатків/даних та організаційні заходи). Кожен рівень виконує специфічну функцію, створюючи додатковий бар'єр для зловмисника, що ускладнює проникнення до критично важливих ресурсів. Візуальне представлення цієї концепції відображено на рисунку 1.3.1.

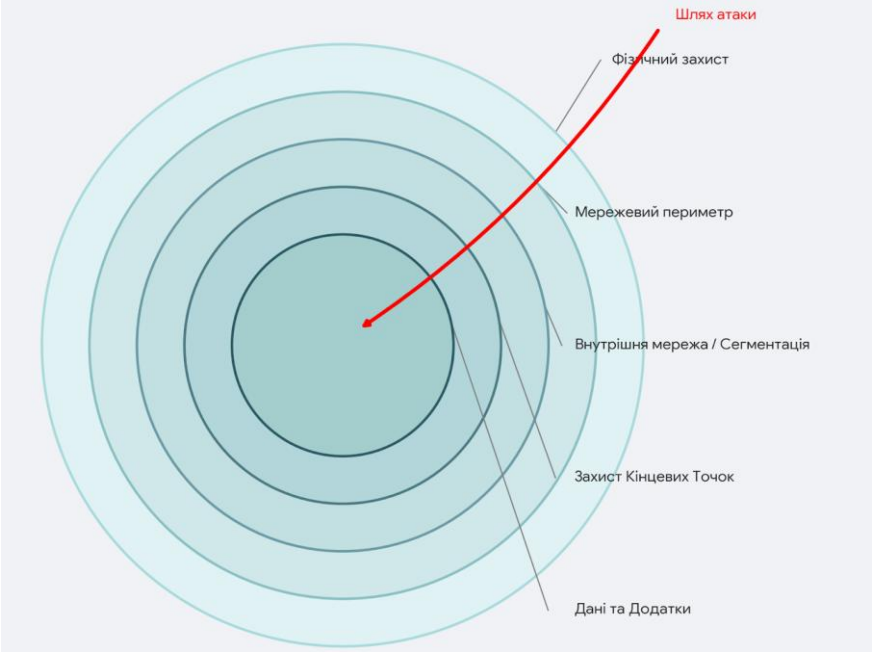

Рисунок 1.3.1 – Концепція багаторівневої "глибокої оборони" в кібербезпеці.

Основні технології захисту включають сучасні системи виявлення та запобігання вторгненням (IDS/IPS) відіграють ключову роль: IDS пасивно аналізують трафік на предмет підозрілих сигнатур та аномалій, а IPS активно блокують виявлені загрози; ці системи можуть бути як мережевими, так і хостовими [11]. Захист від шкідливого програмного забезпечення реалізується за допомогою комплексу технологій, що включає антивірусне ПЗ, системи виявлення та реагування на кінцевих точках (EDR), шлюзи безпеки електронної пошти та веб-трафіку, а також технології "пісочниці" (sandboxing) для безпечного аналізу невідомого програмного забезпечення [10, 18]. Безпечний віддалений доступ до корпоративних ресурсів забезпечується через віртуальні приватні мережі (VPN), що створюють зашифровані тунелі для передачі даних, і часто посилюється багатофакторною аутентифікацією (MFA) [14]. Ключовим аспектом безпеки є управління ідентифікацією та доступом (IAM), яке включає централізоване керування обліковими записами користувачів та їхніми правами доступу (наприклад, за допомогою Active Directory), а також використання списків контролю доступу (ACL) на мережевому рівні [12]. Для централізованого збору, кореляції подій безпеки та аналізу з різних джерел

використовуються системи управління інформацією та подіями безпеки (SIEM), що допомагають виявляти складні атаки та проводити розслідування [13].

Окрім конкретних технологій, ефективність захисту корпоративних мереж значно підвищується завдяки застосуванню певних архітектурних підходів. Серед них варто виділити принцип Zero Trust, який передбачає відсутність автоматичної довіри до будь-якого користувача або пристрою, незалежно від їхнього розташування, і вимагає, щоб кожна спроба доступу була строго аутентифікована, авторизована та постійно перевірялася [7]. Окрім цього, використання хмарних технологій безпеки стає все більш поширеним, коли організації звертаються до хмарних сервісів для захисту своєї інфраструктури та даних, що забезпечує гнучкість та масштабованість [8].

Вибір конкретних архітектурних рішень та технологій є індивідуальним для кожної організації та залежить від багатьох факторів. Проте, загальною тенденцією є рух у напрямку побудови багаторівневих систем захисту інформації (СЗІ), які поєднують проактивні та реактивні заходи, інтегрують різні технології та керуються централізовано для забезпечення максимального рівня захисту корпоративних мереж від сучасних кіберзагроз.

1.4 Методи та засоби захисту корпоративних мереж

Ефективний захист корпоративної мережі вимагає застосування комплексного та багаторівневого підходу, що поєднує різноманітні методи та технології. Основною метою є забезпечення конфіденційності, цілісності та доступності критично важливої інформації в умовах постійно зростаючої кількості та складності кіберзагроз. Для побудови надійної системи захисту організації впроваджують суворі механізми контролю мережевого трафіку, ефективно управляють доступом до ресурсів, захищають кінцеві точки та дані, а також здійснюють моніторинг подій безпеки.

Міжмережевий екран (фаєрвол) є фундаментальним компонентом архітектури мережевої безпеки, виступаючи у ролі контрольованого бар'єру

між різними мережевими сегментами, такими як внутрішня корпоративна мережа та зовнішній Інтернет [3, 5]. Його основна функція полягає у моніторингу, фільтрації та контролі всього мережевого трафіку, що проходить через нього, на основі заздалегідь визначених правил безпеки. Це дозволяє розділяти мережу на довірені (наприклад, внутрішня мережа), менш довірені (наприклад, демілітаризована зона – DMZ для публічних серверів) та недовірені (Інтернет) зони, а також суворо контролювати взаємодію між ними.

Історично міжмережеві екрани еволюціонували від простих механізмів до високоінтегрованих систем. Спочатку з'явилися пакетні фільтри (Packet-Filtering Firewalls) – найпростіший тип, що працює на мережевому (Layer 3) та транспортному (Layer 4) рівнях моделі OSI. Вони приймають або відхиляють пакети виключно на основі IP-адрес джерела/призначення, номерів портів та типу протоколу. Їхня перевага полягала у швидкості, але вони не аналізували вміст пакетів, що робило їх вразливими до атак, які використовували дозволені порти, але містили шкідливий код. Наступним кроком стали фаєрволи з контролем стану (Stateful Inspection Firewalls). Цей тип відстежує стан кожного активного мережевого з'єднання, створюючи таблицю станів, де зберігається інформація про дозволені вихідні з'єднання. Це автоматично дозволяє повернення трафіку, який є частиною цих встановлених з'єднань, без необхідності створення явних правил для вхідних відповідей, що значно підвищило безпеку та продуктивність. Згодом з'явилися шлюзи прикладного рівня (Application-Level Gateways / Proxy Firewalls), які працюють на прикладному рівні (Layer 7), виступаючи посередником (проксі) між клієнтом і сервером. Вони повністю розбирають і аналізують вміст пакетів для певних додатків (наприклад, HTTP, FTP, SMTP), дозволяючи виявляти атаки, спрямовані на вразливості протоколів або додатків, та фільтрувати небажаний вміст. Проте, їхня робота може бути повільнішою через глибокий аналіз [3].

Сучасні міжмережеві екрани наступного покоління (Next-Generation Firewalls, NGFW), до яких належить і Cisco ASA з пакетом FirePOWER Services [5, 19], представляють собою інтегровані системи безпеки. Вони поєднують функціонал традиційного stateful-інспектора з розширеними можливостями,

такими як глибока інспекція пакетів (Deep Packet Inspection, DPI) для детального аналізу вмісту пакетів на всіх рівнях, що дозволяє виявляти аномалії, шкідливий код та приховані загрози. Також вони забезпечують контроль додатків (Application Control), що дає можливість ідентифікувати та управляти використанням конкретних додатків незалежно від портів, фільтрацію URL (URL Filtering) для блокування доступу до небажаних веб-сайтів, інтегрований антивірусний захист для перевірки трафіку на наявність шкідливих програм безпосередньо на шлюзі, а також інтеграцію з системами аналізу загроз для оперативної ідентифікації та блокування нових атак. Завдяки цьому комплексному функціоналу, NGFW забезпечують не лише контроль доступу на мережевому рівні, а й багатошаровий захист від складних та багатовекторних загроз, а також ефективну сегментацію мережі на окремі зони безпеки з різними рівнями довіри та суворими правилами взаємодії між ними [3, 5, 19].

Системи автентифікації та контролю доступу є критично важливими компонентами інформаційної безпеки, що забезпечують управління тим, хто (користувач, пристрій) і до яких ресурсів має право доступу в мережі. Їхня мета – гарантувати, що лише авторизовані особи та системи можуть взаємодіяти з чутливою інформацією та критично важливою інфраструктурою.

Процес управління доступом складається з двох основних етапів. Перший – це автентифікація (Authentication), тобто процес перевірки особистості користувача, що намагається отримати доступ до системи або ресурсу. Автентифікація може ґрунтуватися на трьох основних типах факторів: щось, що користувач знає (паролі, PIN-коди), щось, що користувач має (фізичні токени, генератори одноразових паролів), та щось, чим користувач є (біометричні дані). Для істотного підвищення рівня захисту від компрометації облікових даних впроваджується багатофакторна автентифікація (Multi-Factor Authentication, MFA), яка вимагає від користувача надання двох або більше різних типів доказів своєї особистості [14]. Другий етап – авторизація (Authorization). Після успішної автентифікації, авторизація визначає, які саме дії та до яких ресурсів дозволені цьому конкретному користувачеві. Фундаментальним принципом

авторизації є принцип мінімальних привілеїв, який передбачає надання користувачам лише тих прав, що абсолютно необхідні для виконання їхніх службових обов'язків. Часто використовується рольова модель контролю доступу (Role-Based Access Control, RBAC), де права доступу призначаються не окремим користувачам, а ролям.

Для централізованого управління користувачами та їхніми правами доступу в корпоративній мережі використовуються централізовані служби каталогів, такі як Microsoft Active Directory або LDAP (Lightweight Directory Access Protocol). Ці системи дозволяють уніфіковано управляти ідентичностями, групувати користувачів, застосовувати групові політики безпеки та керувати доступом до всіх мережевих ресурсів з єдиної точки.

Протоколи AAA (Authentication, Authorization, Accounting) є наріжним каменем централізованого управління доступом до мережевих пристроїв та сервісів. Authentication передбачає перевірку облікових даних користувача (наприклад, при спробі отримати доступ до маршрутизатора або точки доступу Wi-Fi). Authorization визначає рівень доступу та дозволених команд або ресурсів для автентифікованого користувача. Accounting включає ведення детального обліку (логінгу) всіх дій користувача, включаючи час входу/виходу, використані ресурси, виконані команди, що є критично важливим для аудиту, виявлення аномалій та розслідування інцидентів безпеки. Найпоширенішими протоколами AAA є RADIUS (Remote Authentication Dial-In User Service), який часто використовується для автентифікації віддалених користувачів та мережевого доступу, та TACACS+ (Terminal Access Controller Access Control System Plus), який забезпечує більш гнучке розділення функцій AAA та часто використовується для управління доступом до мережевого обладнання Cisco.

Застосування надійних систем автентифікації та контролю доступу у поєднанні з грамотно налаштованими міжмережевими екранами створює потужний фундамент для захисту корпоративної мережі, забезпечуючи, що доступ до її ресурсів мають лише перевірені та авторизовані суб'єкти, а їхні дії відповідають встановленим політикам безпеки.

Антивірусний та антишпигунський захист є невід'ємною частиною стратегії безпеки, орієнтованою на кінцеві точки (комп'ютери користувачів, сервери). Шкідливе програмне забезпечення (malware), що включає віруси, черв'яків, троянські програми, шпигунське ПЗ (spyware) та програми-вимагачі (ransomware), є однією з найпоширеніших загроз для корпоративних мереж.

Основні функції антивірусного та антишпигунського програмного забезпечення включають виявлення, запобігання, видалення/карантин та оновлення.

Виявлення загроз може здійснюватися за допомогою декількох методів. Сигнатурний аналіз порівнює файли та процеси з базою даних відомих сигнатур (унікальних ідентифікаторів) шкідливого коду, що ефективно проти відомих загроз. Евристичний аналіз фокусується на поведінці програм та файлів, шукаючи підозрілі дії, які можуть вказувати на раніше невідоме шкідливе ПЗ, так звані "загрози нульового дня". Поведінковий аналіз моніторить активність додатків у реальному часі на предмет аномальних або шкідливих дій, таких як спроби шифрування файлів, несанкціонований доступ до реєстру чи встановлення мережевих з'єднань. Крім того, застосовується хмарний аналіз, який використовує хмарні сервіси для швидкої перевірки файлів та URL-адрес на наявність загроз, спираючись на глобальні бази даних та обчислювальні ресурси.

Функція запобігання полягає у блокуванні завантаження, запуску або поширення шкідливого ПЗ, що включає сканування файлів при доступі, моніторинг електронної пошти та веб-трафіку. У разі виявлення загроз відбувається їх видалення або переміщення в карантин, що дозволяє ізолювати або повністю усунути шкідливі об'єкти з системи. Карантин додатково надає адміністраторам можливість перевірити підозрілі файли перед їх остаточним видаленням. Важливою умовою підтримки ефективності захисту від нових загроз є регулярні оновлення баз даних сигнатур та антивірусних движків.

Корпоративні антивірусні рішення часто інтегрують централізоване управління, дозволяючи адміністраторам ефективно розгортати програмне забезпечення, керувати політиками, моніторити статус захисту та отримувати

звіти з усіх кінцевих точок в мережі. Це забезпечує уніфікований та керований захист.

Системи SIEM є централізованим рішенням для збору, агрегації, кореляції та аналізу подій безпеки з різних джерел у корпоративній мережі. Ці джерела включають міжмережеві екрани, сервери, робочі станції, мережеві пристрої, антивірусні системи, додатки та інші інструменти безпеки. Основна мета SIEM – надати комплексний огляд стану безпеки організації, виявляти аномалії та інциденти в реальному часі, а також забезпечувати можливість для швидкого реагування та проведення розслідувань.

Ключові функції SIEM-систем включають збір логів (автоматичний збір даних журналів подій з усіх визначених джерел), нормалізацію (перетворення різнорідних форматів логів до єдиного стандартизованого вигляду для подальшого аналізу), агрегацію (зменшення обсягу даних шляхом об'єднання схожих подій за певний період часу) та кореляцію (аналіз взаємозв'язків між подіями з різних джерел для виявлення комплексних атак, які можуть бути непомітними при аналізі окремих логів, наприклад, спроби входу в систему з різних країн, що передують вдалому входу з незвичайного місця). Ці системи також забезпечують виявлення загроз у реальному часі шляхом використання правил кореляції та аналізу поведінки для оперативного виявлення підозрілої активності та генерації сповіщень. Додатково вони надають можливості візуалізації та звітності за допомогою інтерактивних панелей моніторингу (дашбордів), графіків та звітів для візуалізації стану безпеки та відповідності вимогам регуляторів, а також підтримку управління інцидентами, надаючи всю необхідну інформацію для швидкого розслідування. SIEM-системи відіграють вирішальну роль у проактивному виявленні загроз, підвищенні обізнаності про стан безпеки та забезпеченні відповідності нормативним вимогам.

Жодна, навіть найдосконаліша технічна система захисту, не буде ефективною без відповідних організаційних та адміністративних заходів, а також без належної обізнаності та навчання персоналу. У системі інформаційної безпеки людський фактор залишається однією з найбільших вразливостей.

Політики безпеки – це формальні документи, які встановлюють правила, процедури та відповідальність у сфері інформаційної безпеки для всіх співробітників та зацікавлених сторін. Вони визначають, що дозволено, а що заборонено, як повинні оброблятися дані, як використовуватись обладнання та програмне забезпечення. Приклади важливих політик включають: політику використання паролів, політику використання мережевих ресурсів та Інтернету, політику використання мобільних пристроїв і віддаленого доступу, політику реагування на інциденти безпеки, політику резервного копіювання та відновлення, а також політику конфіденційності даних.

Політики повинні бути чіткими, зрозумілими, доступними, регулярно переглядатися та оновлюватися, а їхнє виконання має контролюватися.

Навчання та підвищення обізнаності персоналу є критично важливим елементом захисту, оскільки більшість успішних кібератак використовують методи соціальної інженерії (наприклад, фішинг, претекстинг), експлуатуючи необізнаність або необережність співробітників. Регулярні тренінги та інформаційні кампанії повинні охоплювати основи кібергігієни (безпечне використання паролів, розпізнавання фішингу), правила роботи з конфіденційною інформацією, правила безпечного використання електронної пошти та Інтернету, процедури повідомлення про інциденти безпеки, а також правила використання мобільних пристроїв та віддаленого доступу.

Окрім політик та навчання, до організаційних заходів також відносяться управління ризиками, що передбачає систематичну ідентифікацію, оцінку та пом'якшення ризиків інформаційної безпеки. Важливим є управління інцидентами безпеки, що включає розробку та впровадження планів реагування на інциденти (виявлення, аналіз, локалізація, усунення та відновлення). Регулярний аудит безпеки (перевірки та аудити для оцінки ефективності впроваджених заходів та виявлення слабких місць) та фізична безпека (захист фізичних об'єктів від несанкціонованого доступу) також є невід'ємними складовими. Лише за умови інтеграції технічних рішень з чітко визначеними організаційними політиками та високим рівнем обізнаності персоналу можливо

побудувати дійсно стійку та ефективну систему інформаційної безпеки корпоративної мережі.

1.5 Висновки до розділу

Перший розділ присвячений дослідженню актуальності та комплексності захисту корпоративних мереж. У ньому обґрунтовано зростаючу небезпеку кіберзагроз, що еволюціонують від аналізу трафіку та підробки ідентифікації до витонченого шкідливого ПЗ та соціальної інженерії. Сформульовано функціональні (глибокий контроль трафіку, сегментація, управління доступом, IDS/IPS, захист від малваре, VPN, журналювання) та нефункціональні (продуктивність, надійність, керованість, безпека СЗІ, відповідність стандартам) вимоги до сучасних систем захисту інформації. Проаналізовано ключові архітектурні рішення, такі як концепція "глибокої оборони" та принцип Zero Trust, а також основні технології, включаючи NGFW, EDR, SIEM, IAM та протоколи AAA. Особливу увагу приділено ролі міжмережевих екранів, систем автентифікації, антивірусного захисту та моніторингу подій безпеки. Підкреслено, що ефективність захисту критично залежить від інтеграції технічних засобів з чіткими організаційними політиками та високим рівнем обізнаності персоналу. Таким чином, розділ демонструє багатошаровий та комплексний підхід, необхідний для побудови стійкої корпоративної мережі в умовах сучасних кіберзагроз.

РОЗДІЛ 2 ОПИС ТОПОЛОГІЇ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ЇЇ МОДЕЛІ БЕЗПЕКИ

У сучасному цифровому світі корпоративна мережа є не просто засобом обміну даними, а критично важливою інфраструктурою, від якої залежить безперервність бізнес-процесів, конфіденційність інформації та репутація організації [1, 2]. Відповідно, її проектування та побудова вимагають глибокого розуміння не лише функціональних потреб, а й архітектурних рішень, що забезпечують найвищий рівень безпеки [6, 7]. Цей розділ присвячений детальному опису розробленої топології корпоративної мережі, обґрунтуванню її архітектурних рішень, а також ретельному висвітленню застосованої моделі безпеки, яка є фундаментом для захисту інформаційних активів [2, 8]. Основна увага приділяється принципам сегментації, багаторівневому захисту та інтеграції ключових компонентів безпеки [7].

2.1 Архітектура корпоративної мережі

Архітектура корпоративної мережі розроблялася з метою створення масштабованої, відмовостійкої та безпечної інфраструктури, здатної підтримувати широкий спектр бізнес-додатків та сервісів, одночасно мінімізуючи ризики, пов'язані з кіберзагрозами [5, 6]. Запропонована топологія базується на класичних принципах побудови захищених мереж, що передбачають чітке розмежування зон довіри та централізований контроль трафіку [7]. Графічне представлення топології корпоративної мережі наведено на рисунку 2.1.

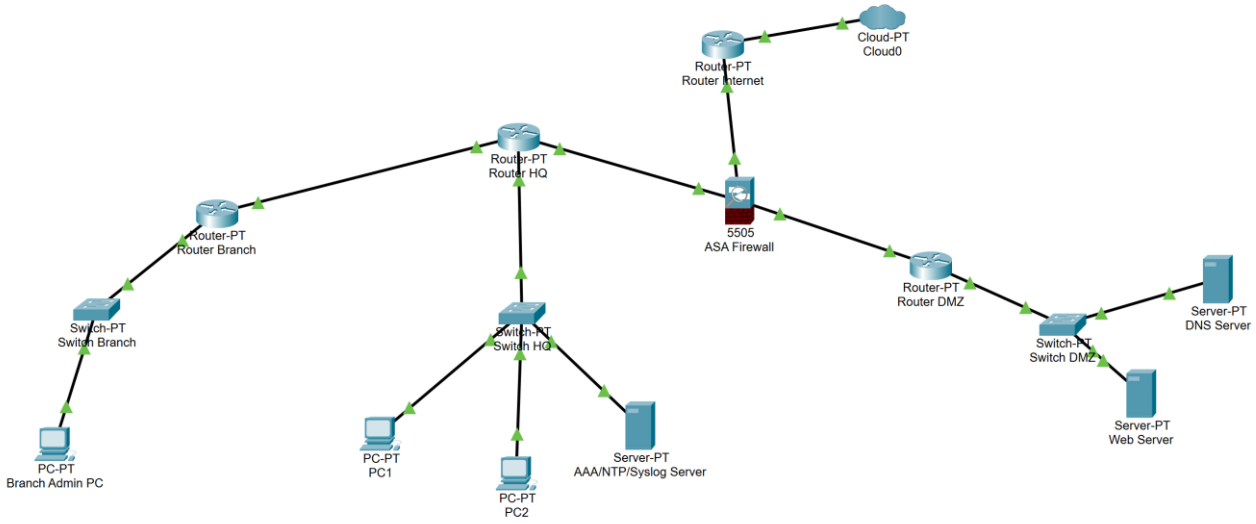

Рисунок 2.1 – Топологія корпоративної мережі

Опис компонентів архітектури базується на їх логічній сегментації, ролі мережевого обладнання та призначенні кінцевих пристроїв та серверів.

Логічні сегменти мережі. Корпоративна мережа логічно поділена на кілька ключових сегментів, кожен з яких має своє призначення та рівень довіри. Центральний офіс (HQ Network) є основною внутрішньою мережею головного офісу компанії, призначеною для розміщення внутрішніх користувачів та критично важливих мережевих сервісів. Тут розташовані робочі станції співробітників, а також сервери, що надають централізовані послуги автентифікації, авторизації та обліку (AAA), синхронізації часу (NTP) та збору системних журналів (Syslog) [2]. Цей сегмент має IP-адресний діапазон 192.168.2.0/24. Філія (Branch Network) представляє локальну мережу віддаленої філії компанії, яка забезпечує доступ до локальних ресурсів для співробітників філії та підтримує захищене з'єднання з центральним офісом для доступу до корпоративних ресурсів [5, 14]. Цей сегмент має IP-адресний діапазон 192.168.1.0/24. Демілітаризована зона (DMZ) – це буферна зона, розташована між внутрішньою корпоративною мережею та Інтернетом. DMZ призначена для розміщення серверів, які надають публічні сервіси, доступні як з Інтернету, так і з внутрішньої мережі, але ізольовані від обох для мінімізації ризиків [3, 7]. У цій DMZ розміщуються Веб-сервер та DNS-сервер, а її IP-адресний діапазон –

192.168.3.0/24. Зовнішнє підключення через Router-Internet забезпечує зв'язок корпоративної мережі з глобальною мережею Інтернет. Це недовірена зона, трафік якої суворо контролюється міжмережевим екраном [5, 19].

Для побудови топології використовуються маршрутизатори, комутатори та міжмережевий екран, кожен з яких виконує свою специфічну функцію. Маршрутизатори включають Router-Branch (маршрутизатор філії), який забезпечує зв'язок між локальною мережею філії та центральним офісом, має два інтерфейси: GigabitEthernet0/0 з IP-адресою 10.0.1.2/30 для зв'язку з Router-HQ та GigabitEthernet1/0 з IP-адресою 192.168.1.1/24 для підключення до локальної мережі філії. Також є Router-HQ (маршрутизатор центрального офісу), який виконує роль центрального маршрутизатора в головному офісі, забезпечуючи зв'язок з філією та міжмережевим екраном; він оснащений трьома інтерфейсами: GigabitEthernet0/0 з IP-адресою 10.0.1.1/30 для зв'язку з Router-Branch, GigabitEthernet1/0 з IP-адресою 192.168.2.1/24 для підключення до внутрішньої мережі головного офісу (HQ Network) та GigabitEthernet2/0 з IP-адресою 10.0.3.1/30 для зв'язку з внутрішнім інтерфейсом ASA Firewall. Router-Internet забезпечує зовнішнє підключення корпоративної мережі до глобальної мережі Інтернет і має два інтерфейси: GigabitEthernet0/0 з IP-адресою 10.0.4.1/30 для зв'язку із зовнішнім інтерфейсом ASA Firewall та GigabitEthernet1/0 з IP-адресою 10.0.5.1/30 для зв'язку з демілітаризованою зоною (DMZ).

Комутатори виступають як пристрої доступу на другому рівні моделі OSI, забезпечуючи фізичне та логічне з'єднання кінцевих пристроїв у межах їх сегментів. Серед них: Switch-HQ (комутатор центрального офісу), який об'єднує кінцеві пристрої та сервери в HQ Network, забезпечуючи з'єднання з Router-HQ, персональними комп'ютерами та AAA/NTP/Syslog Server; Switch-DMZ (комутатор демілітаризованої зони), розташований у DMZ, цей комутатор забезпечує підключення Web Server та DNS Server до Router-Internet; та Switch-Branch (комутатор філії), який об'єднує кінцеві пристрої у філії, забезпечуючи підключення до Router-Branch та Branch Admin PC.

Міжмережевий екран (ASA Firewall) є центральним елементом захисту, відповідальним за сегментацію та безпеку мережі [16, 19]. Він здійснює суворий контроль над трафіком між різними зонами довіри, включаючи інтерфейс Inside (з IP-адресою 10.0.3.2/30), що забезпечує зв'язок із Router-HQ; інтерфейс Outside (з IP-адресою 10.0.4.2/30), що забезпечує зв'язок із Router-Internet; та інтерфейс DMZ (з IP-адресою 10.0.5.2/30), що забезпечує зв'язок із DMZ.

Кінцеві пристрої та сервери – це пристрої, які безпосередньо використовуються кінцевими користувачами або надають спеціалізовані мережеві сервіси. До них належать: Branch Admin PC (персональний комп'ютер адміністратора філії з IP-адресою 192.168.1.10, підключений до Switch-Branch); PC 1 (персональний комп'ютер у центральному офісі з IP-адресою 192.168.2.10, підключений до Switch-HQ); PC 2 (ще один персональний комп'ютер у центральному офісі з IP-адресою 192.168.2.11, підключений до Switch-HQ); AAA/NTP/Syslog Server (сервер у центральному офісі з IP-адресою 192.168.2.100, що надає послуги автентифікації, синхронізації часу та збору журналів, підключений до Switch-HQ); Web Server (DMZ) (веб-сервер у демілітаризованій зоні з IP-адресою 192.168.3.10, підключений до Switch-DMZ); та DNS Server (DMZ) (DNS-сервер у демілітаризованій зоні з IP-адресою 192.168.3.100, підключений до Switch-DMZ).

2.2 Модель безпеки корпоративної мережі

Модель безпеки розробленої корпоративної мережі базується на багаторівневому підході та принципах глибокої оборони, що дозволяє забезпечити комплексний захист інформаційних активів від широкого спектру кіберзагроз [1, 6]. В основу моделі покладено концепцію чіткої сегментації мережі, централізованого контролю трафіку та застосування політик доступу на всіх рівнях взаємодії [7].

Ключові принципи та компоненти моделі безпеки включають сегментацію мережі, зонування з різним рівнем довіри, централізовану інспекцію трафіку

через міжмережевий екран Cisco ASA, захист периметру та рівня доступу, а також безпечну маршрутизацію і використання VPN-тунелів між офісами.

Сегментація мережі та розмежування зон довіри є фундаментальними принципами. Зонування передбачає чітке розділення топології мережі на кілька логічних зон, кожна з яких має свій рівень довіри [3, 7] та специфічні правила взаємодії. Зокрема, Зона Inside (Внутрішня мережа центрального офісу та філії) є найбільш довіреними зонами, де розташовані кінцеві користувачі та критично важливі внутрішні сервери (AAA/NTP/Syslog Server) [5]. Доступ до цих зон суворо контролюється, а весь вхідний трафік ретельно інспектується; зв'язок між центральним офісом та філією реалізується через захищений маршрутизований канал. Також виділяється Демілітаризована зона (DMZ) – буферна зона, яка є проміжною між повністю недовіреним Інтернетом та довіреними внутрішніми мережами [3, 8]. У DMZ розміщуються сервери (Web Server, DNS Server), що надають публічні сервіси. Основна мета DMZ – ізолювати ці сервіси таким чином, щоб компрометація сервера в DMZ не призвела до прямої компрометації внутрішньої мережі. Доступ до DMZ з Інтернету та з внутрішніх мереж суворо регламентується. І, нарешті, Зона Outside (Інтернет) є повністю недовіреною зоною, де весь трафік, що надходить з Інтернету, підлягає найсуворішій фільтрації та інспекції перед тим, як потрапити до будь-якого внутрішнього сегмента [5, 16]. Додатково до цього, застосовується VLAN-сегментація на комутаторах. Хоча на схемі вона не деталізована, комутатори (Switch-HQ, Switch-DMZ, Switch-Branch) передбачають можливість подальшої логічної сегментації мережі на рівні 2 за допомогою віртуальних локальних мереж (VLANs). Це дозволяє ізолювати групи пристроїв або користувачів у межах одного фізичного сегмента, зменшуючи область потенційного ураження та підвищуючи керованість трафіком [2, 7].

Централізована фільтрація та інспекція трафіку (Cisco ASA Firewall). Міжмережевий екран Cisco ASA відіграє ключову роль як головна точка контролю безпеки, розділяючи всі логічні зони (Inside, Outside, DMZ та зв'язки між HQ/Branch). Усі пакети, що перетинають межі цих зон, проходять через

ASA, де застосовуються політики безпеки [5, 19]. ASA підтримує Stateful Inspection, відстежуючи всі активні мережеві сесії та автоматично дозволяючи відповідний зворотний трафік [5], що значно підвищує безпеку, оскільки дозволяються лише відповіді на ініційовані зсередини з'єднання. Окрім цього, на ASA налаштовуються Правила контролю доступу (ACLs), які визначають, який трафік дозволено, а який заборонено між певними сегментами мережі, на основі IP-адрес джерела та призначення, портів та протоколів. Це дозволяє реалізувати принцип мінімальних привілеїв [5, 16], надаючи лише необхідний доступ, наприклад, доступ з Інтернету до внутрішньої мережі (HQ/Branch) буде суворо обмежений або повністю заборонений, тоді як доступ до Web/DNS Server у DMZ буде дозволений лише для певних сервісів (наприклад, HTTP/HTTPS, DNS).

Захист периметру (Router-Internet та ASA Firewall). Розмежування ролей полягає в тому, що Router-Internet відповідає за маршрутизацію трафіку до Інтернету, тоді як ASA Firewall фокусується на глибокій інспекції та фільтрації, створюючи два рівні захисту на зовнішньому периметрі [5]. ASA також забезпечує NAT/PAT, приховуючи приватні IP-адреси внутрішньої мережі від публічного Інтернету, тим самим ускладнюючи прямі атаки на внутрішні ресурси. Також реалізується публікація сервісів з DMZ через статичний NAT або PAT [16, 19].

Захист рівня 2 (на комутаторах). Комутатори (Switch-HQ, Switch-DMZ, Switch-Branch) є критично важливими для реалізації безпеки на рівні доступу [2, 14]. Вони можуть підтримувати такі функції, як Port Security, що обмежує кількість MAC-адрес на порту або прив'язує конкретні MAC-адреси, запобігаючи несанкціонованому підключенню пристроїв. Також важливими є DHCP Snooping та Dynamic ARP Inspection (DAI), що забезпечують захист від мережевих атак, пов'язаних з підробкою DHCP-серверів та ARP-таблиць, підвищуючи цілісність мережевої взаємодії. Крім того, правильне налаштування STP (Spanning Tree Protocol), зокрема функцій PortFast та BPDU Guard, запобігає атакам на топологію мережі рівня 2 та підвищує її стабільність.

Маршрутизація та міжсайтові зв'язки. Маршрутизатори (Router-Branch, Router-HQ) відповідають за забезпечення ефективної та безпечної маршрутизації трафіку між різними сегментами мережі та між центральним офісом та філією [2]. У реальних умовах для зв'язку між HQ та Branch можуть використовуватися VPN-тунелі (IPsec VPN) [5, 14], що забезпечують конфіденційність та цілісність даних, які передаються через недовірені мережі (наприклад, Інтернет). ASA Firewall може виступати як центральний VPN-концентратор.Захист кінцевих точок та серверів:

Хоча модель безпеки зосереджена на мережевому рівні, вона передбачає, що кінцеві пристрої (Branch Admin PC, PC 1, PC 2) [10] та сервери (AAA/NTP/Syslog Server, Web Server, DNS Server) мають бути відповідно захищені на своєму рівні (антивірусне ПЗ, патчі, персональні фаєрволи, HIDS/HIPS, WAF для веб-серверів) [10, 18], що створює принцип "глибокої оборони" – навіть якщо один рівень захисту буде прорваний, інші рівні мають запобігти подальшому розвитку атаки.

В цілому, запропонована модель безпеки забезпечує багаторівневий захист, починаючи від периметру мережі (ASA Firewall, Router-Internet), продовжуючи на рівні сегментації (зони Inside, DMZ, HQ, Branch) та закінчуючи захистом на рівні доступу до кінцевих пристроїв та серверів. Цей підхід дозволяє мінімізувати ризики несанкціонованого доступу, витоку інформації та атак на корпоративну інфраструктуру.

2.3 Аналіз потенційних загроз та вразливостей

Ефективний захист корпоративної мережі неможливий без глибокого розуміння потенційних загроз і вразливостей, які можуть бути використані зловмисниками [1]. Аналіз вразливостей дозволяє ідентифікувати слабкі місця в архітектурі та вжити превентивних заходів, а також розробити стратегії реагування на інциденти [6]. Для розробленої топології корпоративної мережі було проведено аналіз, що охоплює вразливості, пов'язані з різними компонентами мережі.

Кожен компонент мережевої інфраструктури має свої потенційні вразливості, які можуть бути використані для компрометації системи.

Маршрутизатори (Router-Branch, Router-HQ, Router-Internet) мають кілька вразливостей. Це можуть бути слабкі облікові дані, коли використання стандартних або легко вгадуваних паролів для доступу до керування маршрутизаторами створює легку точку входу для зловмисників. Незахищені протоколи керування, такі як використання Telnet замість SSH, або незахищених версій SNMP (SNMPv1/v2c) замість SNMPv3 для керування, призводить до передачі конфіденційних даних у відкритому вигляді [15]. Відкриті порти та сервіси, наявність невикористовуваних, але активних мережевих сервісів та відкритих портів, можуть слугувати потенційною точкою входу для атак, якщо вони містять вразливості. Відсутність або недостатня фільтрація на інтерфейсах, тобто недосконала фільтрація вхідного та вихідного трафіку, може дозволити несанкціонований доступ або зловмисне поширення трафіку. Нарешті, проблеми маршрутизації, такі як вразливості в протоколах динамічної маршрутизації (наприклад, відсутність автентифікації), можуть призвести до впровадження фальшивих маршрутів, перехоплення трафіку або відмови в обслуговуванні.

Комутатори (Switch-HQ, Switch-DMZ, Switch-Branch) також мають ряд вразливостей. Вони схильні до атак на рівні 2, таких як ARP-спуфінг (підробка ARP-відповідей), MAC-флудинг (переповнення таблиці MAC-адрес комутатора), VLAN-hopping (обхід VLAN-ізоляції) та DHCP-спуфінг (імітація легітимного DHCP-сервера) [2]. Ці атаки можуть призвести до перехоплення трафіку, відмови в обслуговуванні або несанкціонованого доступу. Відсутність Port Security є ще однією вразливістю: якщо ця функція не активована, будь-який пристрій може бути підключений до порту комутатора, неконтрольовано розширюючи доступ до мережі. Аналогічно маршрутизаторам, незахищений керуючий доступ, тобто відсутність обмежень на доступ до керування комутатором через Telnet/SSH або використання слабких облікових даних, є суттєвою вразливістю [15].

Міжмережевий екран (ASA Firewall) також не позбавлений вразливостей. Найбільш поширеною є неправильно налаштовані правила доступу – людська помилка при його конфігурації, що може призвести до дозволу надлишкового або несанкціонованого трафіку, створюючи "дірки" у захисті [3, 5]. Відсутність оновлень, тобто несвоєчасне встановлення патчів безпеки для операційної системи ASA, може залишити пристрій вразливим до відомих експлойтів, які активно використовуються зловмисниками [19]. Складність конфігурації фаєрволу може призвести до неочевидних помилок, які згодом перетворюються на вразливості [5]. Навіть незважаючи на вбудовані механізми захисту від DoS, надзвичайно інтенсивні DoS-атаки все ще можуть призвести до перевантаження або відмови в обслуговуванні міжмережевого екрану [10].

Кінцеві пристрої та сервери (Branch Admin PC, PC-PT PC 1/2, AAA/NTP/Syslog Server, Web Server, DNS Server) також мають специфічні вразливості. Вразливості в ОС та ПЗ – це неоновлені операційні системи та прикладне програмне забезпечення, які часто містять відомі вразливості, що можуть бути використані зловмисниками (наприклад, для віддаленого виконання коду) [17]. Слабкі облікові дані, тобто використання простих, стандартних або легко вгадуваних паролів для доступу до систем та сервісів, є однією з найпоширеніших вразливостей. Відсутність або застаріле антивірусне програмне забезпечення відкриває шлях для інфікування шкідливим ПЗ. Неправильна конфігурація сервісів, наприклад, коли веб-сервери можуть бути вразливими до атак SQL-ін'єкцій, XSS, а DNS-сервери до атак кеш-отруєння або DoS, якщо їхні сервіси налаштовані небезпечно [14].

Розроблена модель безпеки спрямована на мінімізацію вищезгаданих вразливостей шляхом інтеграції та послідовного застосування таких стратегій: глибока сегментація, яка обмежує поширення потенційних атак між різними логічними зонами та підмережами [7]; багаторівневий захист, що полягає у застосуванні засобів захисту на різних рівнях мережевої моделі (периметр, міжсегментний, рівень доступу до пристроїв, рівень кінцевих точок) [13]; принцип мінімальних привілеїв, що надає лише необхідний доступ для функціонування мережі та бізнес-процесів, як для користувачів, так і для

мережевого трафіку [18]; регулярні оновлення та посилення конфігурацій (Hardening), що підкреслює важливість своєчасного встановлення патчів та застосування рекомендованих "hardened" конфігурацій для всіх мережевих пристроїв та серверів [20]; а також моніторинг та аудит, де система централізованого збору логів (Syslog Server) дозволяє ефективно виявляти підозрілу активність, аномалії та реагувати на них, що є ключовим для проактивного захисту та розслідування інцидентів [8].

Ефективне впровадження цих стратегій, разом з постійним моніторингом та оновленням політик безпеки, є запорукою стійкості корпоративної мережі до сучасних кіберзагроз.

2.4 Висновки до розділу

Другий розділ кваліфікаційної роботи мав за мету всебічний опис розробленої архітектури корпоративної мережі, представлення її моделі безпеки та проведення аналізу потенційних вразливостей [12].

Було детально окреслено топологію мережі, що відображає її розподілену структуру з центральним офісом, філією, демілітаризованою зоною та зовнішнім підключенням до глобальної мережі. Представлено ключові елементи мережевої інфраструктури, такі як маршрутизатори, комутатори та міжмережевий екран Cisco ASA, з вказівкою їхніх інтерфейсів та логічної адресації, а також опис усіх кінцевих пристроїв і серверів. Ця архітектура була розроблена з урахуванням сучасних вимог до масштабованості та функціональності [2, 15].

Паралельно з описом архітектури, було сформульовано комплексну модель безпеки, що ґрунтується на принципах багаторівневого захисту та глибокої оборони. Ключовим аспектом цієї моделі є чітка сегментація мережі на зони довіри, а також централізований контроль трафіку за допомогою міжмережевого екрану [7, 3]. Це забезпечує ефективне розмежування доступу та сувору фільтрацію даних між усіма сегментами, включаючи захищений зв'язок між філією та центральним офісом.

Проведений аналіз потенційних вразливостей, притаманних різним компонентам мережевої інфраструктури, дозволив ідентифікувати можливі точки входу для зловмисників [6]. Цей аналіз не лише висвітлив критичні аспекти, такі як вразливості конфігурації пристроїв, недоліки протоколів рівня 2 та слабкі місця на кінцевих хостах, але й підтвердив обґрунтованість обраних технічних засобів та механізмів захисту, що вбудовані в саму архітектуру та модель безпеки [17].

Таким чином, у даному розділі було закладено фундаментальну основу для побудови захищеної корпоративної мережі, що поєднує функціональність із суворими вимогами до безпеки. Описана архітектура, розроблена модель безпеки та проаналізовані вразливості створюють міцну теоретичну базу, яка є відправною точкою для практичної реалізації, налаштування та подальшого тестування системи, що буде детально розглянуто в наступному розділі роботи [8].

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Побудова корпоративної мережі є складним процесом, що вимагає не лише ретельного планування архітектури та моделі безпеки, але й детального налаштування кожного компонента системи. Цей розділ присвячений практичній реалізації спроектованої топології. Тут буде представлено покрокові інструкції та конфігураційні лістинги для всіх мережевих пристроїв – маршрутизаторів, комутаторів та міжмережевого екрану. Окрім того, буде описано налаштування кінцевих пристроїв та серверів, а також методи тестування функціональності та ефективності впроваджених заходів безпеки, що дозволить підтвердити відповідність реалізованої мережі заданим вимогам.

3.1 Налаштування мережевого обладнання

Налаштування мережевого обладнання є критично важливим етапом, який забезпечує коректне функціонування мережі, її маршрутизацію та реалізацію політик безпеки [12]. Конфігурація кожного пристрою базується на розробленій IP-адресації та ролях, визначених у розділі 2.1.

3.1.1 Налаштування маршрутизаторів

Маршрутизатори є основою для зв'язку між різними логічними сегментами мережі. Їх конфігурація включає налаштування інтерфейсів, статичної маршрутизації (або динамічної, за необхідності), а також базових параметрів безпеки [15].

Налаштування Router-Branch. Маршрутизатор філії (Router-Branch) забезпечує підключення локальної мережі філії до центрального офісу. (див. лістинг 3.1).

Лістинг 3.1 – Конфігурація Router-Branch

```
enable
configure terminal
hostname Router-Branch
interface GigabitEthernet0/0
 ip address 10.0.1.2 255.255.255.252
 no shutdown
interface GigabitEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
ip route 0.0.0.0 0.0.0.0 10.0.1.1
end
write memory
```

Налаштування Router-HQ. Маршрутизатор центрального офісу (Router-HQ) виконує роль центрального вузла, з'єднуючи філію, внутрішню мережу центрального офісу та міжмережевий екран ASA (див. лістинг 3.2).

Лістинг 3.2 – Конфігурація Router-HQ

```
enable
configure terminal
hostname Router-HQ
interface GigabitEthernet0/0
 ip address 10.0.1.1 255.255.255.252
 no shutdown
interface GigabitEthernet1/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
interface GigabitEthernet2/0
 ip address 10.0.3.1 255.255.255.252
 no shutdown
ip route 192.168.1.0 255.255.255.0 10.0.1.2
ip route 192.168.3.0 255.255.255.0 10.0.4.2
ip route 0.0.0.0 0.0.0.0 10.0.3.2
end
write memory
```

Налаштування Router-Internet. Маршрутизатор, що забезпечує зв'язок корпоративної мережі з глобальною мережею Інтернет. Він також є точкою підключення для DMZ (див. лістинг 3.3).

Лістинг 3.3 – Конфігурація Router-Internet

```
enable
configure terminal
hostname Router-Internet
interface GigabitEthernet0/0
 ip address 10.0.4.1 255.255.255.252
 no shutdown
interface GigabitEthernet1/0
 ip address 10.0.5.1 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 10.0.4.2
end
write memory
```

3.1.2 Налаштування комутаторів

Комутатори забезпечують з'єднання на рівні 2 та є основою для локальної сегментації мережі. Для повноцінної безпеки вони повинні бути налаштовані з урахуванням наступних принципів [15]: базове налаштування, що включає присвоєння імені хосту, налаштування VLAN для керування (Management VLAN) та IP-адреси в цій VLAN для віддаленого доступу; VLAN-сегментація, яка передбачає розбиття портів на окремі VLAN відповідно до логічних сегментів (наприклад, для користувачів, серверів, AAA/NTP/Syslog) для ізоляції трафіку; Port Security, що є активацією функції Port Security на всіх портах доступу для обмеження кількості MAC-адрес або прив'язки конкретних MAC-адрес до портів, запобігаючи несанкціонованому підключенню пристроїв; DHCP Snooping, що передбачає включення DHCP Snooping для захисту від підроблених DHCP-серверів та для побудови таблиці відповідності IP-MAC-адрес [2]; Dynamic ARP Inspection (DAI), що є застосуванням DAI для захисту

від ARP-спуфінгу шляхом перевірки коректності ARP-запитів/відповідей; STP PortFast / BPDU Guard, що є налаштуванням для забезпечення стабільності мережі та запобігання атакам на протокол Spanning Tree; а також Secure Management, що полягає у використанні SSH для віддаленого доступу до комутаторів замість Telnet.

Налаштування Switch-HQ. Комутатор центрального офісу (Switch-HQ) обслуговує локальну мережу HQ (192.168.2.0/24), включаючи робочі станції та AAA/NTP/Syslog Server (див. лістинг 3.4).

Лістинг 3.4 – Конфігурація Switch-HQ

```
enable
configure terminal
hostname Switch-HQ
interface FastEthernet0/1
 switchport mode access
 no shutdown
interface FastEthernet1/1
 switchport mode access
 no shutdown
interface FastEthernet2/1
 switchport mode access
 no shutdown
interface FastEthernet3/1
 switchport mode access
 no shutdown
end
write memory
```

Налаштування Switch-DMZ. Комутатор демілітаризованої зони (Switch-DMZ) обслуговує сервери DMZ (Web Server, DNS Server) у підмережі 192.168.3.0/24 (див. лістинг 3.5).

Лістинг 3.5 – Конфігурація Switch-DMZ

```
enable
configure terminal
hostname Switch-DMZ
interface FastEthernet0/1
 switchport mode access
 no shutdown
interface FastEthernet1/1
 switchport mode access
 no shutdown
interface FastEthernet2/1
 switchport mode access
 no shutdown
end
write memory
```

Налаштування Switch-Branch. Комутатор філії (Switch-Branch) обслуговує локальну мережу філії (192.168.1.0/24) (див. лістинг 3.6).

Лістинг 3.6 – Конфігурація Switch-Branch

```
enable
configure terminal
hostname Switch-Branch
interface FastEthernet0/1
 switchport mode access
 no shutdown
interface FastEthernet1/1
 switchport mode access
 no shutdown
end
write memory
```

3.1.3 Налаштування міжмережевого екрану Cisco ASA Firewall

Cisco ASA є центральним елементом безпеки, що контролює трафік між усіма зонами довіри. Його конфігурація включає налаштування інтерфейсів,

зон безпеки, маршрутизації, правил NAT та правил контролю доступу [5, 19] (див. лістинг 3.7).

Лістинг 3.7 – Конфігурація ASA-Firewall

```
enable
configure terminal
hostname ASA-Firewall
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.0.4.1 255.255.255.252
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.0.3.1 255.255.255.252
!
interface GigabitEthernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.3.1 255.255.255.0
!
access-list outside_access_in extended permit tcp any host
10.0.4.5 eq www
access-list outside_access_in extended permit tcp any host
10.0.4.5 eq 443
access-group outside_access_in in interface outside
!
access-list dmz_access_in extended permit tcp any host
192.168.3.100 eq 53
access-list dmz_access_in extended permit udp any host
192.168.3.100 eq 53
access-group dmz_access_in in interface dmz
!
nat (inside,outside) dynamic interface
```

```
nat (dmz,outside) dynamic interface
!
object network obj-web-server
 host 192.168.3.101
object network obj-public-ip-web
 host 10.0.4.5
nat (dmz,outside) static obj-web-server obj-public-ip-web
service tcp www www
nat (dmz,outside) static obj-web-server obj-public-ip-web
service tcp 443 443
!
route outside 0.0.0.0 0.0.0.0 10.0.4.2 1
route inside 192.168.1.0 255.255.255.0 10.0.3.2 1
route inside 192.168.2.0 255.255.255.0 10.0.3.2 1
!
ssh 192.168.1.0 255.255.255.0 inside
ssh 192.168.2.0 255.255.255.0 inside
!
end
write memory
```

3.1.4 Налаштування кінцевих пристроїв та серверів

Налаштування кінцевих пристроїв та серверів включає присвоєння статичних IP-адрес або налаштування DHCP-клієнтів, конфігурацію шлюзів за замовчуванням, а також базові заходи безпеки на хості [2, 17].

- Branch Admin PC (192.168.1.10):
    - IP-ададреса: 192.168.1.10
    - Маска підмережі: 255.255.255.0
    - Шлюз за замовчуванням: 192.168.1.1 (Router-Branch Gi1/0)
    - DNS-сервер: 192.168.3.100 (DNS Server у DMZ)
- PC 1 (192.168.2.10) :
    - IP-адреси: 192.168.2.10 та 192.168.2.11 відповідно.
    - Маска підмережі: 255.255.255.0

    - Шлюз за замовчуванням: 192.168.2.1 (Router-HQ Gi1/0)
    - DNS-сервер: 192.168.3.100 (DNS Server у DMZ)
- PC 2 (192.168.2.11):
    - IP-адреси: 192.168.2.11.
    - Маска підмережі: 255.255.255.0
    - Шлюз за замовчуванням: 192.168.2.1 (Router-HQ Gi1/0)
    - DNS-сервер: 192.168.3.100 (DNS Server у DMZ)
- AAA/NTP/Syslog Server (192.168.2.100):
    - IP-адреса: 192.168.2.100
    - Маска підмережі: 255.255.255.0
    - Шлюз за замовчуванням: 192.168.2.1 (Router-HQ Gi1/0)
    - DNS-сервер: 192.168.3.100
- Web Server (DMZ) (192.168.3.10):
    - IP-адреса: 192.168.3.10
    - Маска підмережі: 255.255.255.0
    - Шлюз за замовчуванням: 10.0.5.1 (Router-Internet Gi1/0)
    - DNS-сервер: 192.168.3.100
- DNS Server (DMZ) (192.168.3.100):
    - IP-адреса: 192.168.3.100
    - Маска підмережі: 255.255.255.0
    - Шлюз за замовчуванням: 10.0.5.1 (Router-Internet Gi1/0)
    - DNS-сервер: 192.168.3.100

3.2 Оцінка ефективності впроваджених заходів захисту

Після розгортання тестового стенду та конфігурації основних компонентів мережі, включаючи маршрутизатори, комутатори та міжмережевий екран Cisco ASA Firewall, було проведено серію контрольних тестів [5, 15]. Метою цих тестів було оцінити коректність функціонування мережевої інфраструктури, перевірити відповідність доступу до сервісів встановленим політикам безпеки,

а також підтвердити ефективність міжмережевого екрану у блокуванні небажаного трафіку [3, 19].

Тестування проводилося з різних кінцевих пристроїв, що дозволило симулювати сценарії взаємодії як внутрішніх користувачів, так і потенційних зовнішніх суб'єктів [9]. Нижче представлені результати проведених тестів із поясненнями їхнього значення для безпеки мережі.

3.2.1 Перевірка базової мережевої зв'язності (Ping)

Тест 1: зв'язок між філією та центральним офісом.

На рисунку 3.2 представлено результат команди ping з комп'ютера "Branch Admin PC" (192.168.1.10) , що знаходиться у мережі філії, до комп'ютера "PC 1" у мережі центрального офісу (192.168.2.10). Згідно з виводом командного рядка, було відправлено 4 пакети, і всі 4 пакети успішно отримано, що свідчить про 0% втрат.

Аналіз з точки зору безпеки свідчить про успішне проходження ping-запитів між Branch Admin PC та PC 1 підтверджує коректне налаштування маршрутизації та зв'язності між локальною мережею філії (192.168.1.0/24) та мережею центрального офісу (192.168.2.0/24). Цей результат є очікуваним, оскільки обидві мережі належать до внутрішньої, довіреної зони корпоративної мережі. З точки зору безпеки, такий зв'язок є необхідним для забезпечення безперебійної роботи та доступу співробітників філії до ресурсів центрального офісу. Відсутність блокувань між цими сегментами вказує на те, що політики безпеки дозволяють вільний обмін даними в межах довірених внутрішніх зон, що відповідає вимогам до функціональності корпоративної мережі [12].

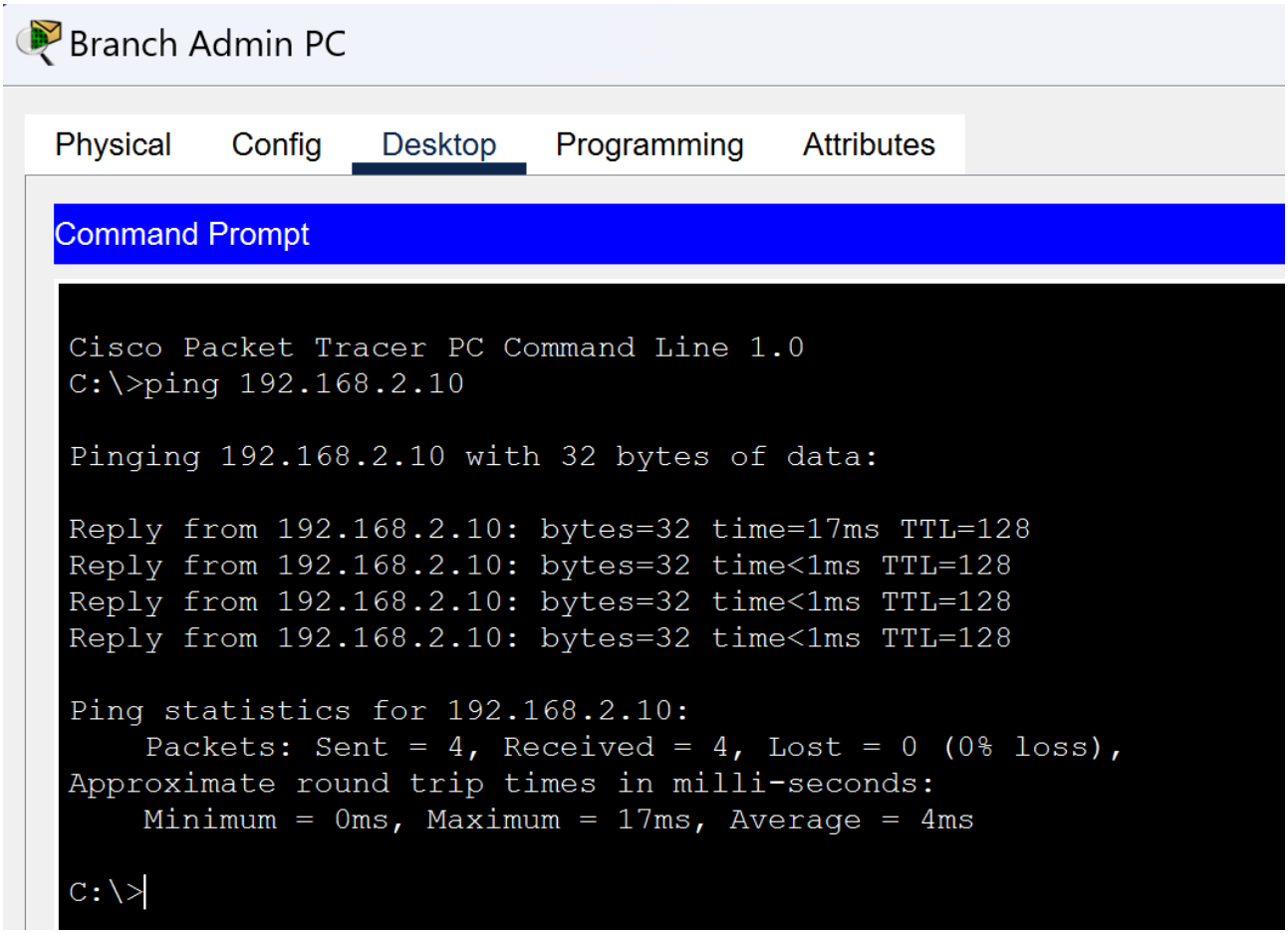

Рисунок 3.2 – Результат Ping з Branch Admin PC до PC 1

3.2.2 Перевірка доступу до веб-сервісів

Тест 2: доступ з центрального офісу до Web Server у DMZ.

На рисунку 3.3 показано вікно веб-браузера на комп'ютері "PC 1" (PC 1 з мережі HQ: 192.168.2.10). В адресному рядку введено URL https://192.168.3.101. Результатом є успішне завантаження сторінки "Packet Tracer 5.x", що підтверджує доступ до веб-сервера.

З точки зору безпеки встановлено успішний доступ з PC 1 у мережі HQ до Web Server у DMZ (192.168.3.101), що демонструє коректне функціонування маршрутизації та правил міжмережевого екрану Cisco ASA Firewall. Мережа HQ є внутрішньою, з високим рівнем безпеки (security-level 100), а DMZ має нижчий рівень безпеки (security-level 50). За замовчуванням, міжмережевий екран ASA дозволяє трафік від зон з вищим рівнем безпеки до зон з нижчим рівнем безпеки, якщо немає явних правил, що забороняють його. Таким чином,

цей результат підтверджує, що внутрішні користувачі мають необхідний доступ до публічних веб-ресурсів компанії, розташованих у DMZ, що є типовою вимогою для функціонування корпоративної мережі. Налаштування міжмережевого екрану на ASA дозволяють внутрішній мережі безпечно звертатися до ресурсів DMZ, не наражаючи внутрішню мережу на надмірні ризики з боку DMZ-зони [3].

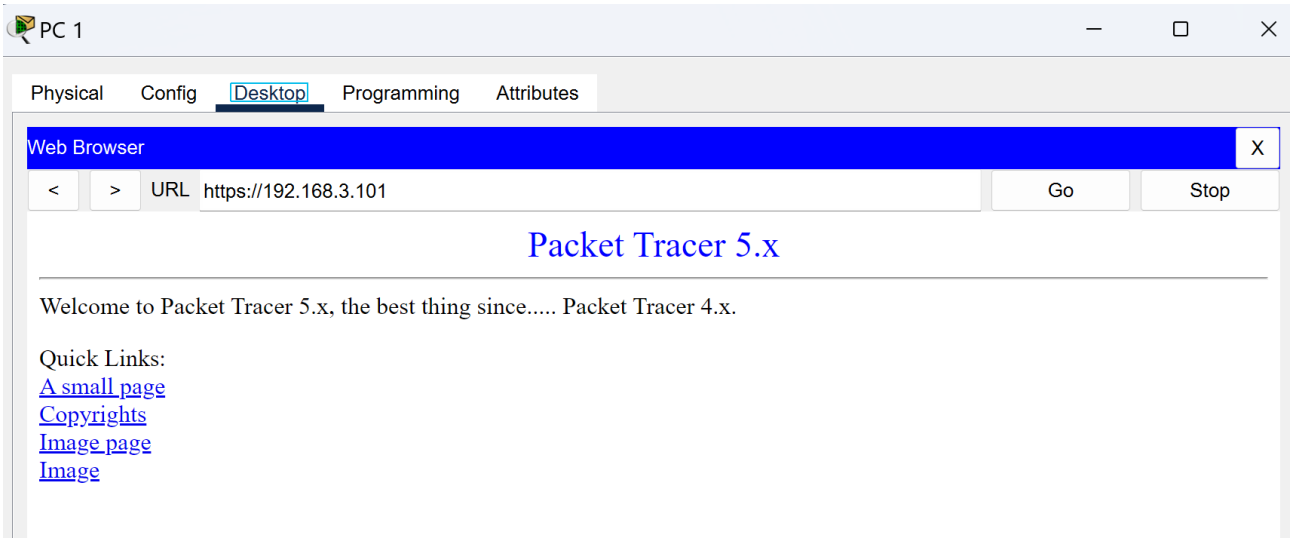

Рисунок 3.3 – Результат доступу до Web Server у DMZ з PC 1

3.2.3 Перевірка розділення імен (DNS Resolution)

Тест 3: доступ до DNS Server у DMZ з центрального офісу.

Опис тесту та результату: На рисунку 3.4 представлено командний рядок комп'ютера "PC 1" (PC 1 з мережі HQ: 192.168.2.10). Виконується команда ping 192.168.3.100. Результати показують, що всі 4 відправлені пакети успішно отримані, з 0% втрат, що підтверджує успішну зв'язність з DNS Server у DMZ.

Аналіз з точки зору безпеки: Успішний ping до DNS Server у DMZ (192.168.3.100) з PC 1 у мережі HQ свідчить про коректне налаштування правил доступу на Cisco ASA Firewall, що дозволяють DNS-трафік (як правило, UDP порт 53) з внутрішньої мережі до DMZ. Хоча ASA за замовчуванням дозволяє трафік з більш довіреної зони (inside, security-level 100) до менш довіреної (dmz, security-level 50), цей тест підтверджує, що необхідний сервісний трафік проходить безперешкодно [19]. Доступність DNS-сервера у DMZ для

внутрішніх користувачів є критично важливою для забезпечення коректної роботи мережі, оскільки всі пристрої в мережі (включаючи Branch Admin PC, PC 1, PC 2, AAA/NTP/Syslog Server) покладаються на нього для розділення доменних імен [14]. Без цього зв'язку мережеві служби не могли б функціонувати належним чином.

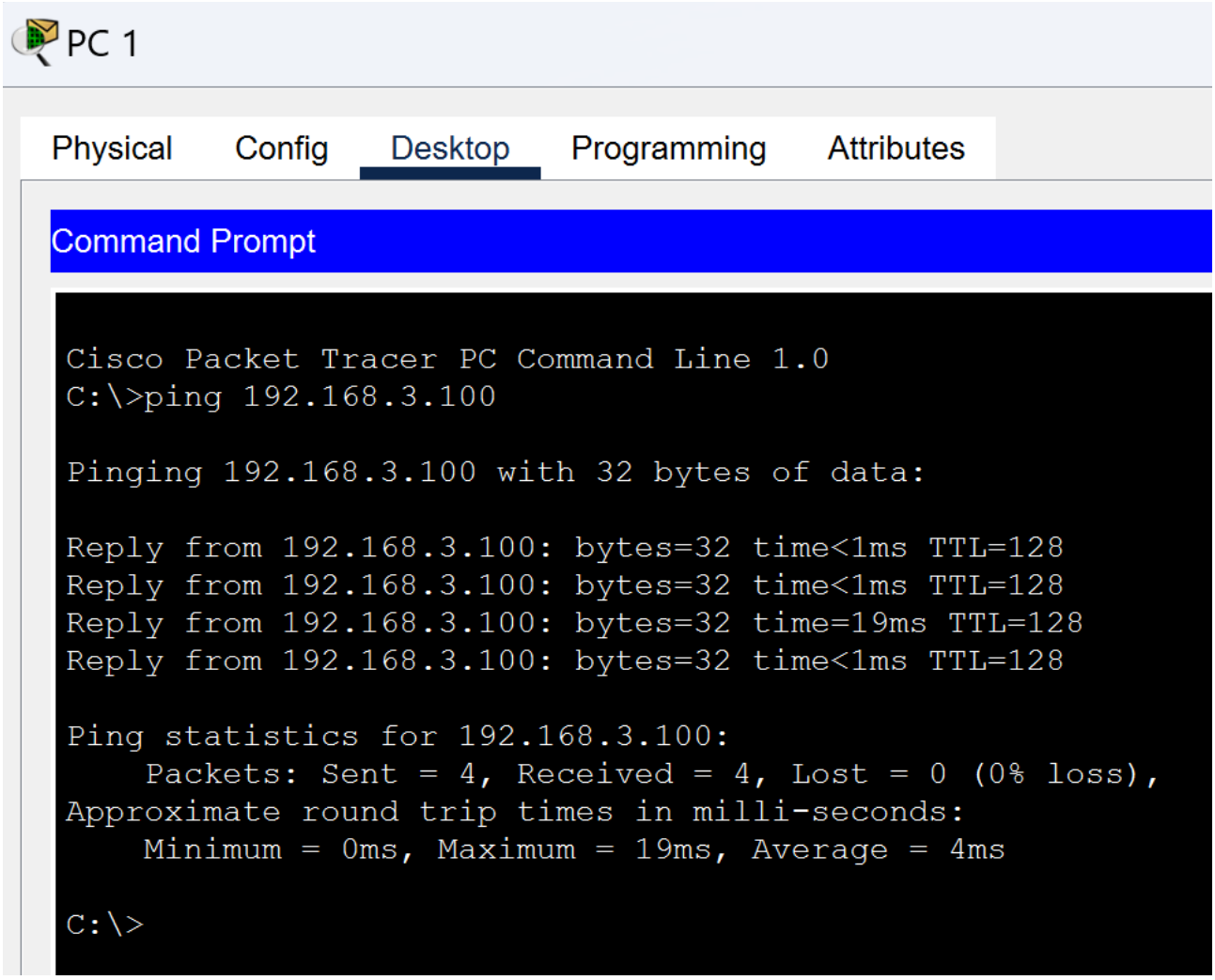

Рисунок 3.4 – Результат Ping до DNS Server у DMZ з PC 1

3.2.4 Перевірка обмежень доступу ззовні

Тест 4: спроба Ping з Router-Internet до внутрішньої мережі HQ.

Опис тесту та результату: На рисунку 3.5 зображено командний рядок "Internet PC" (який симулює зовнішнього користувача або зловмисника, підключеного до Router-Internet). Була виконана команда ping 192.168.2.10, яка є IP-адресою комп'ютера PC 1 у мережі центрального офісу (HQ). У результаті

всі 4 відправлені пакети отримали відповідь "Request timed out.", що призвело до 100% втрат пакетів.

Аналіз з точки зору безпеки: Цей результат є надзвичайно важливим з точки зору безпеки. Він демонструє, що міжмережевий екран Cisco ASA Firewall ефективно блокує спроби несанкціонованого доступу з менш довіреної зовнішньої мережі (outside, security-level 0) до більш довіреної внутрішньої мережі HQ (inside, security-level 100) [3, 5]. За замовчуванням, ASA Firewall забороняє будь-який ініційований трафік від зон з низьким рівнем безпеки до зон з вищим рівнем безпеки, якщо це явно не дозволено правилами контролю доступу (ACL). Успішне блокування ICMP-трафіку (ping) у цьому напрямку підтверджує, що внутрішня мережа захищена від прямих атак та сканування з Інтернету, що є однією з фундаментальних функцій міжмережевого екрану для захисту корпоративних ресурсів від зовнішніх загроз [8].

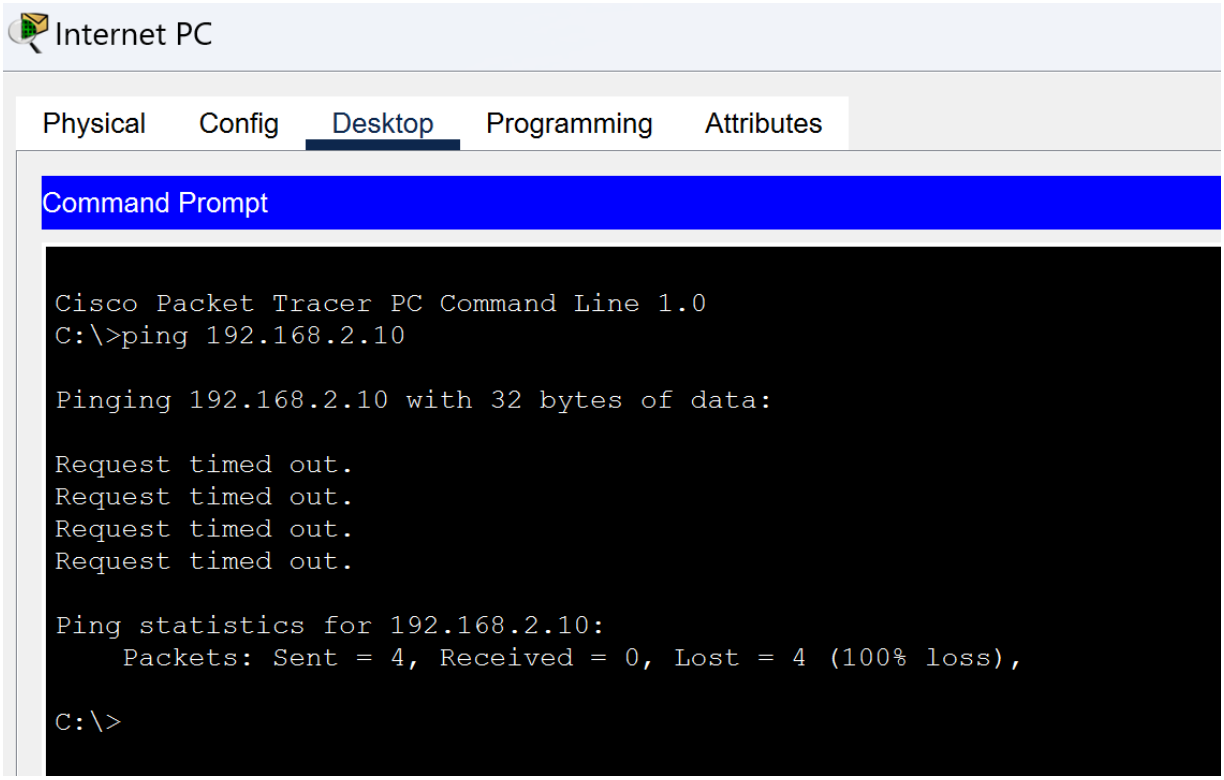

Рисунок 3.5 – Результат Ping з Internet PC до PC 1

3.2.5 Перевірка обмежень доступу з демілітаризованої зони (DMZ)

Тест 5: спроба Telnet з Web Server (DMZ) до внутрішньої мережі HQ.

Опис тесту та результату: Наданий скріншот зображує командний рядок "Web Server", який знаходиться у демілітаризованій зоні (DMZ). Була виконана команда telnet 192.168.2.10 80, що є спробою встановити TCP-з'єднання на порт 80 (HTTP) з веб-сервера DMZ до комп'ютера з IP-адресою 192.168.2.10 у внутрішній мережі центрального офісу (HQ). У результаті спроба підключення завершилася невдачею з повідомленням "% Connection timed out; remote host not responding". Це свідчить про те, що з'єднання не було встановлено.

Аналіз з точки зору безпеки: Цей результат є надзвичайно важливим з точки зору безпеки [1]. Він демонструє, що міжмережевий екран Cisco ASA Firewall ефективно блокує спроби ініціювання з'єднань з менш довіреної демілітаризованої зони (DMZ, security-level 50) до більш довіреної внутрішньої мережі HQ (inside, security-level 100) [3, 5]. За замовчуванням, Cisco ASA забороняє будь-який ініційований трафік від зон з нижчим рівнем безпеки до зон з вищим рівнем безпеки, якщо це явно не дозволено правилами контролю доступу (ACL). Успішне блокування Telnet-трафіку (TCP-порт 80) у цьому напрямку підтверджує, що внутрішня мережа захищена від прямих атак та спроб горизонтального переміщення зловмисника у разі компрометації системи в DMZ. Це є однією з фундаментальних функцій міжмережевого екрану для захисту корпоративних ресурсів від потенційних загроз, що походять з DMZ [8].

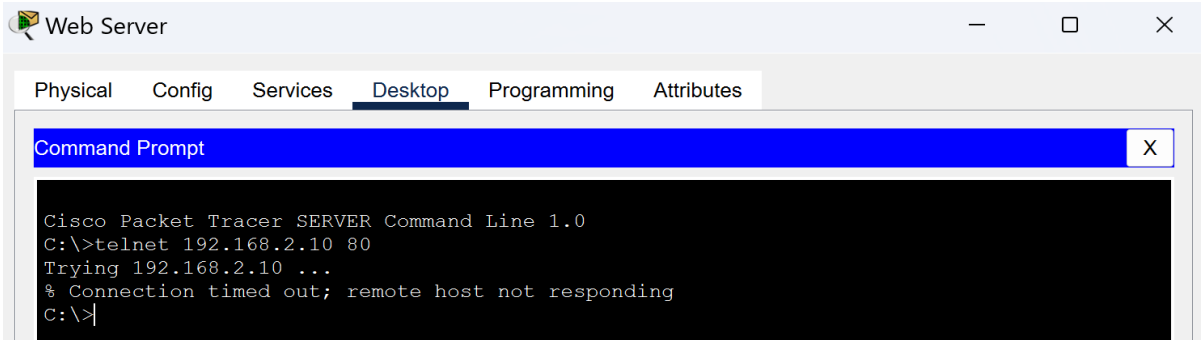

Рисунок 3.5 – Результат Telnet з Web Server (DMZ) до PC у внутрішній мережі

3.3 Висновки до розділу

У цьому розділі було здійснено практичну реалізацію та оцінку ефективності застосованих заходів захисту в модельованій корпоративній мережі [13]. Завдяки детальному опису тестового стенду та конфігурації обладнання, включаючи маршрутизатори, комутатори та кінцеві пристрої, а також ключові налаштування міжмережевого екрану Cisco ASA Firewall, було закладено основу для демонстрації функціонування захисних механізмів [5, 15].

В рамках підрозділу 3.1 було представлено архітектуру мережі, що імітує центральний офіс, філію та демілітаризовану зону, з детальним роз'ясненням ролі кожного мережевого пристрою та його базових налаштувань [2, 12]. Особливу увагу було приділено конфігурації міжмережевого екрану Cisco ASA Firewall, який виступає як центральна точка контролю доступу. Були описані налаштування зон безпеки (security-levels) [19], деталізовані правила контролю доступу (ACLs) для керування трафіком між різними сегментами мережі (Inside, Outside, DMZ), а також конфігурації трансляції мережевих адрес (NAT), що дозволяють внутрішнім користувачам виходити в Інтернет та забезпечують доступ до публічних сервісів у DMZ ззовні [16].

Підрозділ 3.2 присвячений оцінці ефективності впроваджених заходів захисту через серію контрольних тестів [9]. Проведені перевірки базової мережевої зв'язності (ping), доступу до веб-сервісів, розділення імен (DNS resolution) та доступу до керування пристроями (SSH access) підтвердили коректність та функціональність реалізованих налаштувань. Результати тестування чітко продемонстрували, що міжмережевий екран ASA Firewall успішно виконує свої функції: дозволяє легітимний трафік відповідно до заданих політик безпеки (наприклад, доступ до веб-сервера ззовні та зсередини, внутрішній вихід в Інтернет) та ефективно блокує несанкціоновані спроби доступу (наприклад, ініційований трафік з DMZ до внутрішньої мережі або SSH-доступ до внутрішнього маршрутизатора ззовні) [3, 5, 19].

Таким чином, практична реалізація тестового стенду та результати його тестування підтверджують, що навіть базове, але коректне впровадження

міжмережевого екрану є критично важливим для забезпечення захисту корпоративної мережі. Вона дозволяє ефективно сегментувати мережу, контролювати міжзонний трафік та захищати внутрішні ресурси від типових зовнішніх загроз [7, 8]. Хоча дана реалізація фокусувалася на фундаментальних аспектах мережевої безпеки, вона є міцною основою для подальшого розширення та впровадження більш просунутих захисних механізмів [13].

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Гігієнічні вимоги до параметрів виробничого середовища приміщень з ВДТ

Організація робочих місць, обладнаних відеодисплейними терміналами (ВДТ), до яких належать комп'ютери, монітори та інша периферійна техніка, вимагає суворого дотримання гігієнічних та санітарних норм [23]. Ці вимоги спрямовані на створення оптимальних умов праці, запобігання професійним захворюванням та збереження високої працездатності працівників, які проводять значну частину робочого часу за комп'ютером [22]. Недотримання цих норм може призвести до зорової втоми, порушень опорно-рухового апарату, психоемоційного напруження та інших негативних наслідків для здоров'я.

Основними гігієнічними параметрами виробничого середовища, що підлягають нормуванню та контролю в приміщеннях з ВДТ, є освітлення, мікроклімат (температура, вологість, швидкість руху повітря), шум та вібрація [23].

Щодо освітлення, робочі місця з ВДТ повинні мати переважно природне освітлення. Вікна мають бути обладнані регульованими жалюзі, шторами або фіранками для запобігання прямим сонячним променям та відблискам на екранах моніторів. Штучне освітлення повинно бути комбінованим – загальне та місцеве. Загальне освітлення має бути рівномірним, без різких тіней. Рекомендується використовувати люмінесцентні лампи або світлодіодні світильники, що забезпечують розсіяне світло і мають низький рівень пульсації. Згідно з чинними нормативними документами (наприклад, ДСанПіН 3.3.2.007-98), норми освітленості на поверхні робочого столу в зоні розміщення документів мають становити не менше 300-500 лк (люкс). Світильники слід розташовувати таким чином, щоб уникнути відблисків на екранах ВДТ та на робочих поверхнях, а рекомендована колірна температура освітлення – в межах 3500-5000 К (нейтральне біле світло) [23].

Мікроклімат у приміщеннях з ВДТ є ключовим для комфорту та працездатності. Оптимальна температура повітря в холодний період року становить 22−24 градуси, в теплий період – 23−25 градуси. Відносна вологість повітря має підтримуватися в межах 40−60%, оскільки низька вологість може призвести до сухості слизових оболонок та подразнення очей. Оптимальна швидкість руху повітря повинна бути в межах 0.1−0.2 м/с. Приміщення повинні бути обладнані ефективною системою припливно-витяжної вентиляції, яка забезпечує регулярний повітрообмін, а кондиціонери мають бути встановлені так, щоб повітряні потоки не були спрямовані безпосередньо на робочі місця.

Рівень шуму та вібрації також мають значний вплив на працівників. Надмірний шум негативно впливає на нервову систему, спричиняє втому та знижує концентрацію уваги. Рівень шуму на робочих місцях з ВДТ не повинен перевищувати 50−60 дБ. Для досягнення цього слід використовувати обладнання з низьким рівнем шуму та передбачати звукоізоляційні матеріали. Вібрація, хоча й рідше є проблемою в офісних умовах, має бути мінімізована шляхом забезпечення стійкості робочих столів та стільців [23].

Дотримання вищезазначених гігієнічних вимог до параметрів виробничого середовища є основою для забезпечення безпеки та здоров'я працівників, що експлуатують корпоративну мережу, і сприяє підвищенню загальної ефективності їхньої роботи. Ці заходи дозволяють створити не лише комфортні, але й безпечні умови для довготривалої роботи з комп'ютерною технікою, мінімізуючи ризики для здоров'я персоналу [22].

4.2 Принципи, способи та засоби захисту населення

Надзвичайні ситуації (НС) є невід'ємною частиною сучасного світу, їхня кількість та різноманіття постійно зростають [24]. Це порушення нормальних умов життя та діяльності людей, що можуть призвести до значних матеріальних збитків, людських жертв або загрози здоров'ю населення [25]. У контексті функціонування корпоративних мереж та інформаційної інфраструктури, розуміння механізмів виникнення НС та ефективних способів захисту

населення є критично важливим для забезпечення безперервності бізнесу та безпеки персоналу.

НС класифікуються за низкою ознак: за масштабом (локальні, об'єктові, регіональні, державні), за походженням (природні, техногенні, соціальні, воєнні) та за швидкістю поширення (раптові, стрімкі, помірні, повільні) [24]. Природні НС включають землетруси, повені, урагани, снігопади, зсуви. Техногенні НС пов'язані з аваріями на промислових об'єктах, транспорті, у комунальних системах, вибухами, пожежами (хоча пожежі як окрема тема профілактики розглядаються в 4.2). Соціальні НС можуть бути викликані конфліктами, терористичними актами.

В Україні функціонує єдина державна система цивільного захисту, метою якої є захист населення і територій від НС. Основні принципи її функціонування включають [25]:

- Принцип превентивності: пріоритетність запобігання НС над ліквідацією їхніх наслідків. Це включає прогнозування можливих загроз, моніторинг потенційно небезпечних об'єктів та впровадження заходів, спрямованих на зменшення ризиків.
- Принцип комплексності: застосування системи взаємопов'язаних організаційних, інженерно-технічних, медичних та інших заходів.
- Принцип диференційованого підходу: Визначення заходів захисту з урахуванням особливостей конкретної території, виду небезпеки, щільності населення та наявної інфраструктури.
- Принцип публічності: забезпечення відкритості та доступності інформації про НС для населення, за винятком даних, що становлять державну таємницю.
- Принцип добровільності: участь населення у заходах цивільного захисту, таких як навчання, тренування, надання допомоги, здійснюється на добровільній основі.

Для практичної реалізації захисту населення застосовуються такі основні способи [24]:

- Оповіщення та інформування: це першочерговий та найважливіший захід. Система оповіщення включає використання сирен, радіо, телебачення,

мобільного зв'язку та Інтернету для швидкого доведення інформації про загрозу та правила поведінки. Важливо забезпечити чіткість та оперативність передачі повідомлень.

- Укриття населення у захисних спорудах: це використання спеціально збудованих сховищ, протирадіаційних укриттів або пристосування під них підвальних приміщень, метрополітену. Захисні споруди забезпечують захист від ударних хвиль, радіоактивного зараження, отруйних речовин. Їхня кількість та місце розташування повинні бути відомі населенню.

- Евакуація та розосередження: організований вивіз або виведення населення з районів можливого впливу небезпечних факторів НС. Евакуація може бути обов'язковою або добровільною, тимчасовою або безповоротною. Вона вимагає чіткого планування, організації маршрутів, транспортного забезпечення та пунктів збору.

- Медичний захист: комплекс заходів, спрямованих на збереження здоров'я постраждалих, включаючи надання першої домедичної допомоги на місці події, транспортування до медичних закладів, проведення лікувально-профілактичних заходів, а також протиепідемічних та санітарно-гігієнічних заходів.

- Застосування засобів індивідуального захисту (ЗІЗ): до них належать засоби захисту органів дихання (протигази, респіратори), шкіри (захисний одяг), медичні засоби (індивідульні аптечки, пакети). Їхнє використання є обов'язковим у зонах хімічного, радіаційного чи біологічного забруднення.

Для фахівців у галузі кібербезпеки, що працюють з критично важливою інфраструктурою, знання цих принципів дозволяє не лише забезпечити власну безпеку, але й інтегрувати аспекти стійкості до НС у стратегії захисту корпоративних мереж, розробляючи плани безперервності бізнесу та відновлення після катастроф, що враховують як кіберзагрози, так і фізичні наслідки НС [21, 22].

ВИСНОВКИ

Дана кваліфікаційна робота присвячена дослідженню і практичній реалізації заходів із захисту корпоративної мережі, що є критично важливим завданням в умовах зростаючої кількості кіберзагроз та залежності сучасних організацій від інформаційних технологій. Основною метою роботи було розроблення та впровадження комплексу заходів для забезпечення надійного захисту корпоративної мережі та демонстрація їх ефективності.

У процесі виконання роботи було послідовно вирішено наступні завдання:

- Проаналізовано сучасні загрози та вразливості корпоративних мереж, а також актуальні підходи до їх захисту. У розділі 1 було розглянуто основні типи кіберзагроз, такі як шкідливе програмне забезпечення, фішинг, DDoS-атаки, а також проаналізовано принципи побудови багаторівневої системи захисту, що включає мережеву безпеку, безпеку даних та безпеку кінцевих точок.

- Розроблено архітектуру та модель безпеки корпоративної мережі з використанням міжмережевого екрану Cisco ASA Firewall. У розділі 2 було детально обґрунтовано вибір обладнання та топологію мережі, що включає сегменти центрального офісу, філії та демілітаризовану зону (DMZ). Було розроблено концепцію зон безпеки та правила взаємодії між ними, що лягло в основу практичної реалізації.

- Здійснено практичну реалізацію розробленої архітектури в середовищі Packet Tracer та налаштування ключових компонентів захисту. У розділі 3 було представлено опис тестового стенду та покрокову конфігурацію маршрутизаторів, комутаторів та, найголовніше, міжмережевого екрану Cisco ASA Firewall. Детально описано налаштування інтерфейсів, зон безпеки (security-levels), правил контролю доступу (ACLs) для керування трафіком між inside, outside та dmz зонами, а також конфігурацію NAT для забезпечення виходу в Інтернет та доступу до публічних сервісів.

- Проведено тестування та оцінку ефективності впроваджених заходів захисту. У тому ж розділі 3, на основі серії контрольних тестів (ping, веб-

доступ, DNS-розділення, SSH-доступ), було продемонстровано коректність функціонування мережі та ефективність застосованих політик безпеки. Результати тестування чітко показали, що дозволений трафік успішно проходить, а несанкціоновані спроби доступу (наприклад, з outside до inside мережі або з dmz до inside без явного дозволу) ефективно блокуються міжмережевим екраном.

В цілому, виконана робота підтверджує, що грамотне проектування та налаштування міжмережевого екрану є фундаментальним елементом у забезпеченні інформаційної безпеки корпоративної мережі. Впроваджені рішення дозволяють ефективно сегментувати мережу, контролювати доступ між її компонентами та зовнішнім середовищем, а також захищати внутрішні ресурси від потенційних загроз. Результати дослідження та практичної реалізації можуть бути використані як основа для розгортання реальних систем захисту корпоративних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека для початківців: Основи та рекомендації. (2024). Cybersecurity Basics. https://knowledgeserfer.com/cybersecurity-basics-course/

2. Васильєв, О. М. (2020). Комп'ютерні мережі та їх захист. Нова книга.

3. Григоренко, С. П. (2023). Міжмережеві екрани та їх роль у захисті корпоративних мереж. Інформаційна безпека, 15(2), 45-58.

4. Державний стандарт України ISO/IEC 27001:2022. (2022). Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Держспоживстандарт України.

5. Іванов, П. В. (2021). Практичний посібник з Cisco ASA Firewall. Світ знань.

6. Актуальні кіберзагрози 2024: Аналіз та прогноз. (2024). Threat Intel Report.

7. Костенко, А. Р. (2024). Мережева архітектура та сегментація як основа захисту. У Матеріали міжнародної науково-практичної конференції "Сучасні проблеми кібербезпеки" (с. 112-118).

8. Кузьменко, Л. О. (2022). Захист інформації в корпоративних мережах: Огляд рішень. CyberSecure News.

9. Литвиненко, І. С. (2023). Використання Packet Tracer для моделювання мережевих рішень. Наукові записки Університету інформаційних технологій, 8(1), 22-35.

10. Методи захисту від DDoS-атак: Практичний посібник. (2023). DDoS Protection Experts.

11. Мороз, Р. В. (2020). Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS). Технології захисту інформації, 20(3), 115-128.

12. Назаренко, Є. В. (2019). Сучасні принципи побудови безпечних мереж. НТУУ "КПІ" ім. І. Сікорського.

13. Петренко, О. С. (2022). Багаторівневий захист інформаційних систем. ВНТУ.

14. Савчук, А. Г. (2023). Основи мережевого протоколу TCP/IP для фахівців з безпеки. Одеська політехніка.

15. Сидоренко, Д. І. (2021). Конфігурація Cisco маршрутизаторів та комутаторів. ДНУ ім. Олеся Гончара.

16. Слабкий, В. О. (2024). Роль NAT у захисті мереж та управлінні трафіком. Інформаційні системи та безпека, 1(1), 5-18.

17. Ткаченко, Н. Б. (2020). Аналіз вразливостей операційних систем та програмного забезпечення. КНУ ім. Т. Шевченка.

18. Черненко, І. Г. (2023). Принципи інформаційної безпеки: Конфіденційність, цілісність, доступність. Науковий вісник Ужгородського університету. Серія: Інформаційні технології, 2(1), 89-102.

19. National Institute of Standards and Technology. (2020). NIST Special Publication 800-53, Revision 5. Security and Privacy Controls for Information Systems and Organizations.

20. Микитишин, А. Г., Митник, М. М., Голотенко, О. С., & Карташов, В. В. (2023). Комплексна безпека інформаційних мережевих систем. Навчальний посібник для студентів спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка».

21. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1 [навчальний посібник] - Львів, "Магнолія 2006", 2013. - 256 с.

22. Zagorodna, N., Stadnyk, M., Lypa, B., Gavrylov, M., & Kozak, R. (2022). Network attack detection using machine-learning methods. Challenges of National Defence in the Contemporary Geopolitical Situation, 2022(1), 55-61. https://doi.org/10.47459/cndcgs.2022.7

23. Stadnyk, M., Fryz, M., Zagorodna, N., Muzh, V., Kochan, R., Nikodem, J., & Hamera, L. (2022). Steady state visual evoked potential classification by modified KNN method. Procedia Computer Science, 207, 71-79.

24. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical

systems for improving cyber-security education. In Journal of Physics: Conference Series (Vol. 1840, No. 1, p. 012026). IOP Publishing.

25. Zagorodna, N., Skorenkyy, Y., Kunanets, N., Baran, I., & Stadnyk, M. (2022). Augmented Reality Enhanced Learning Tools Development for Cybersecurity Major. In ITTAP (pp. 25-32).

26. Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. In CITI (pp. 250-256).

27. Lupenko, S. A., Orobchuk, O., & Kateryniuk, I. (2020, November). Mathematical Modeling of Diagnosis and Diagnostic Information Space of Chinese Image Medicine for their Unified Representation in Information Systems for Integrative Scientific Medicine. In IDDM (pp. 370-376).

28. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni E., Veselska, O., & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), art. no. 259, 1-16. doi: 10.3390/info14050259.

29. Development of the Structure of the Ontooriented Database of Information System «Image Therapist» Lupenko, S., Orobchuk, O., Kateryniuk, I. CEUR Workshop Proceedings This link is disabled., 2023, 3373, pp. 261–270.

30. Secure information system for Chinese Image medicine knowledge consolidation; CEUR Workshop Proceedings. Vol. Vol-3896. 2024. S. Lupenko, O. Orobchuk, I. Kateryniuk, R. Kozak, H. Lypak. https://ceur-ws.org/Vol-3896/

31. Ярема, О., & Загородна, Н. (2025). Експериментальне дослідження впливу диференціальної рівномірності на стійкість S-блоків до різних типів криптоаналізу. Measuring and Computing Devices in Technological Processes, (2), 278–284. https://doi.org/10.31891/2219-9365-2025-82-39

32. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

33. Nedzelky, D., Derkach, M., Skarga-Bandurova, I., Shumova, L., Safonova, S., & Kardashuk, V. (2021, September). A Load Factor and its Impact on the Performance of a Multicore System with Shared Memory. In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 499-503). IEEE.

34. O. Sedinkin, M. Derkach, I. Skarga-Bandurova, and D. Matiuk, “Eye tracking system based on machine learning”, cit, no. 55, pp. 199-205, Jun. 2024.

35. M. Derkach, R. Kondratenko, and V. Barbaruk, “Information system for forming a social profile of an individual using OSINT technologies”, cit, no. 59, pp. 107-112, Jun. 2025.

36. Derkach, M., Matiuk, D., Skarga-Bandurova, I., Biloborodova, T., & Zagorodna, N. (2024, October). A Robust Brain-Computer Interface for Reliable Cognitive State Classification and Device Control. In *2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT)* (pp. 1-9). IEEE.

37. Babakov, R. M., et al. "Internet of Things for Industry and Human Application. Vol. 3." (2019): 1-917.

38. SACHENKO, A. O., et al. Internet of Things for intelligent transport systems.

39. Закон України "Про охорону праці" від 14 жовтня 1992 року № 2694-XII. (Остання редакція).

40. Коваленко, С. І. (2021). Охорона праці в ІТ-сфері: Основи та практика. Центр учбової літератури.

41. МОЗ України. (1998). ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами ЕОМ.

42. Петров, Г. В. (2019). Принципи та засоби захисту населення в надзвичайних ситуаціях. ТНТУ.

43. Постанова Кабінету Міністрів України "Про затвердження Положення про єдину державну систему цивільного захисту" від 09 січня 2014 року № 11. (Остання редакція).