

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту сервісів LLMNR
вузлів Windows-мережі організації»

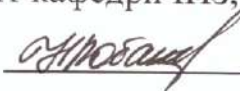
Виконав: студентка 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Ольга БОРДЮГ

Керівник: зав. кафедри КІ та КБ, к.т.н., доц.

 Андрій ЄФІМЕНКО

Рецензент: доцент кафедри ІПЗ, к.т.н., доц.

 Надія ЛОБАНЧИКОВА

Житомир – 2025

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

5 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студентка: Бордюг Ольга Олександрівна

Тема роботи: «Проект підсистеми захисту сервісів LLMNR вузлів Windows-мережі організації»

затверджена Наказом університету від 03 березня 2025 р. № 80 /с.

Термін здачі студентом закінченої роботи 10 червня 2025 р.

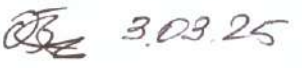
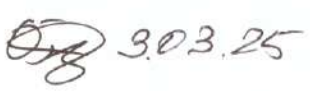
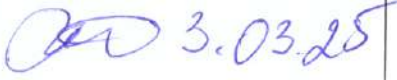
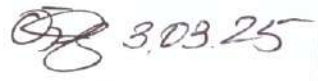
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження виступають процеси захисту вузлів Windows-мережі організації. Предмет дослідження є методи, засоби та технології захисту сервісів LLMNR вузлів Windows-мережі організації.

Обладнання та програмне забезпечення:

1. Персональний комп'ютер з підтримкою віртуалізації (не менше 8 ГБ оперативної пам'яті, процесор з архітектурою x64).
2. Windows Server 2022 (для розгортання Snort, Wireshark).
3. Середовище віртуалізації: Oracle VM VirtualBox 7.0

4. Мережевий симулятор: GNS3 (для побудови та візуалізації топології мережі, емуляції мережевої поведінки).
5. Інструменти для розвідки та тестування: Nmap, Snort.
6. Програмне забезпечення для журналювання та захисту: Snort IDS, Wireshark.
7. Офісні програми: Microsoft Word / LibreOffice Writer (для оформлення звітності), PowerPoint (для підготовки презентації).

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олена ГОЛОВНЯ	 3.03.25	 3.03.25
2	Олена ГОЛОВНЯ	 3.03.25	 3.03.25
3	Олена ГОЛОВНЯ	 3.03.25	 3.03.25

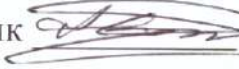
Студент  Ольга БОРДЮГ

Керівник  Андрій ЄФІМЕНКО

Календарний план

№ з/п	Назва етапу виконання ВКР	Термін виконання	Приміт ка
1	Постановка теми, визначення мети, об'єкта і предмета дослідження	05.03 – 15.03	
2	Аналіз літературних джерел та сучасного стану теми	16.03 – 25.03	
3	Формування структури пояснювальної записки	26.03 – 28.03	
4	Моделювання базової корпоративної мережі	29.03 – 10.04	
5	Аналіз загроз безпеки та вразливостей LLMNR-сервісів	11.04 – 20.04	
6	Розробка архітектури захищеної мережевої підсистеми	21.04 – 30.04	
7	Підготовка мережевого середовища та серверної інфраструктури	01.05 – 10.05	
8	Тестування, збір і аналіз результатів	11.05 – 15.05	
9	Оформлення пояснювальної записки	16.05 – 31.05	
10	Перевірка роботи на плагіат, остаточне редагування	01.06 – 05.06	
11	Підготовка презентації та захист	06.06 – 10.06	

Студент  Ольга БОРДЮГ

Керівник  Андрій ЄФІМЕНКО

РЕФЕРАТ

Пояснювальна записка: 73 с., 15 рисунків, 2 таблиці, 23 джерела.

Метою випускної кваліфікаційної роботи є розробка підсистеми захисту сервісів LLMNR вузлів Windows-мережі організації.

У процесі дослідження в межах виконання кваліфікаційної роботи було проведено аналіз протоколу LLMNR, його застосувань в корпоративній інфраструктурі та недоліків безпеки. Здійснено аналіз загроз безпеки та вразливостей LLMNR-сервісів, проектування підсистеми корпоративної мережі та проведено планування заходів безпеки. Проведено вибір обладнання, налаштування та тестування мережі, перевірено тестування підсистеми безпеки та верифікацію захисних заходів. На основі проведених досліджень отримано результати, які демонструють ефективність запропонованої архітектури захисту від LLMNR-атак через комбінацію мережевої сегментації, централізованого моніторингу та контролю доступу. Впровадження технології RSPAN забезпечило значне покращення видимості мережевого трафіку, а фізичне розділення відділів суттєво обмежило можливості латерального переміщення злоумисників. Результати тестування в емуляційному середовищі GNS3 підтвердили зниження ризику компрометації облікових даних, локалізацію потенційних загроз у межах окремих сегментів та підвищення загальної стійкості корпоративної інфраструктури. Розроблені рішення можуть служити основою для створення комплексної системи захисту від атак на протоколи розв'язання імен з акцентом на превентивне виявлення аномальної мережевої активності та швидке реагування на інциденти безпеки.

Ключові слова: WINDOWS-ІНФРАСТРУКТУРА, ЗАХИСТ МЕРЕЖІ, КІБЕРАТАКИ, КОРПОРАТИВНА МЕРЕЖА, LLMNR, МЕРЕЖЕВА БЕЗПЕКА, ТЕСТУВАННЯ БЕЗПЕКИ

					ККІКБ.КР.Б – 125 – 1 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Бордюг О.О.		20.06.25	Проект підсистеми захисту сервісів LLMNR вузлів Windows-мережі організації Пояснювальна записка	Літ.	Арк.
Керівник		Єфіменко А.А.		20.06.25			Аркуші
Реценз.		Лобанчикова Н.		20.06.25			4
Н. контр.		Єфіменко А.А.		20.06.25		ФІКТ, гр. КБ-22-1	
Затверд.		Єфіменко А.А.		20.06.25			

ABSTRACT

Explanatory Note: 73 pages, 15 images, 2 tables, 23 sources.

The objective of this bachelors thesis is to develop a protection subsystem for LLMNR services of Windows network nodes in an organization.

During the research conducted within the scope of this thesis, an analysis of the LLMNR protocol, its applications in corporate infrastructure, and security vulnerabilities was performed. A security threat and vulnerability analysis of LLMNR services was conducted, corporate network subsystem design was carried out, and security measures planning was implemented. Equipment selection, network configuration and testing were performed, security subsystem testing and protective measures verification were conducted. Based on the conducted research, results were obtained that demonstrate the effectiveness of the proposed LLMNR attack protection architecture through a combination of network segmentation, centralized monitoring, and access control. Implementation of RSPAN technology provided significant improvement in network traffic visibility, while physical separation of departments substantially limited lateral movement opportunities for attackers. Testing results in the GNS3 emulation environment confirmed reduced risk of credential compromise, localization of potential threats within separate segments, and increased overall resilience of corporate infrastructure. The developed solutions can serve as a foundation for creating a comprehensive protection system against attacks on name resolution protocols with emphasis on proactive detection of anomalous network activity and rapid incident response.

Keywords: WINDOWS INFRASTRUCTURE, NETWORK PROTECTION, CYBERATTACKS, CORPORATE NETWORK, LLMNR, NETWORK SECURITY, SECURITY TESTING.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ.....	7
ВСТУП.....	8
РОЗДІЛ 1. АНАЛІЗ ПРОТОКОЛУ LLMNR, ЙОГО ЗАСТОСУВАНЬ В КОРПОРАТИВНІЙ ІНФРАСТРУКТУРІ ТА НЕДОЛІКІВ БЕЗПЕКИ	10
1.1. Принципи роботи служб розв'язання імен у Windows-середовищі.....	10
1.2 Протокол LLMNR	12
1.3 Застосування LLMNR у корпоративній інфраструктурі.....	19
Висновки до першого розділу.....	24
РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЛАНУВАННЯ ЗАХОДІВ БЕЗПЕКИ	27
2.1 Механізми експлуатації та сценарії LLMNR-атак.....	27
2.2 Оцінка ризиків для корпоративної інфраструктури	28
2.3 Розробка архітектури захищеної підсистеми мережі	31
Висновки до другого розділу	37
РОЗДІЛ 3. ВДОСКОНАЛЕННЯ МЕТОДІВ РОЗВІДКИ ТА ЗАХИСТУ В КОРПОРАТИВНІЙ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ CYBER KILL CHAIN .	39
3.1 Проектування мережевої архітектури та вибір обладнання	39
3.2 Розгортання мережевої інфраструктури в середовищі GNS3	41
3.3 Конфігурація мережевого обладнання та налаштування моніторингу	44
Висновки до третього розділу.....	51
ВИСНОВКИ	53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	55
ДОДАТКИ.....	57

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ

DNS – Domain Name System (Система доменних імен)

IGMP – Internet Group Management Protocol (Протокол управління групами в Інтернеті)

IP – Internet Protocol (Інтернет-протокол)

IPv4 – Internet Protocol version 4 (Інтернет-протокол версії 4)

IPv6 – Internet Protocol version 6 (Інтернет-протокол версії 6)

LAN – Local Area Network (Локальна мережа)

LLMNR – Link-Local Multicast Name Resolution (Локальне групове розв'язання імен)

mDNS – Multicast Domain Name System (Групова система доменних імен)

MITM – Man-in-the-Middle (Атака "людина посередині")

NBT-NS – NetBIOS Name Service (Служба імен NetBIOS)

NetBIOS – Network Basic Input/Output System (Мережева базова система введення/виведення)

OS – Operating System (Операційна система)

TCP – Transmission Control Protocol (Протокол управління передачею)

UDP – User Datagram Protocol (Протокол користувацьких датаграм)

URL – Uniform Resource Locator (Уніфікований локатор ресурсів)

VLAN – Virtual Local Area Network (Віртуальна локальна мережа)

WAN – Wide Area Network (Глобальна мережа)

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність дослідження. В умовах зростаючої складності корпоративних мереж та активного впровадження Windows-інфраструктур у критично важливих бізнес-процесах питання забезпечення безпеки мережевих сервісів набуває особливої актуальності. Сучасні організації все більше покладаються на автоматизовані системи розв'язання імен для забезпечення безперервної роботи внутрішніх сервісів, обміну даними між підрозділами та доступу до корпоративних ресурсів. У такому середовищі протокол LLMNR (Link-Local Multicast Name Resolution), незважаючи на свою корисність у локальному розв'язанні імен, створює значні ризики для інформаційної безпеки.

Особливу небезпеку становлять LLMNR-атаки, які дозволяють зловмисникам перехоплювати multicast-запити, надавати фальшиві відповіді та захоплювати облікові дані користувачів. Ці атаки можуть призвести до компрометації контролера домену, латерального переміщення в мережі, зловживання довірчими відносинами та повної компрометації Active Directory. Критичність ситуації посилюється тим, що LLMNR функціонує автоматично в Windows-середовищах без додаткового адміністративного втручання, створюючи невидимі вектори атак. У зв'язку з цим актуальним стає розробка комплексних захисних механізмів, які включають мережеву сегментацію, активний моніторинг трафіку, системи виявлення аномальної активності та засоби швидкого реагування на інциденти безпеки.

Метою даної кваліфікаційної роботи є розробка підсистеми захисту сервісів LLMNR вузлів Windows-мережі організації.

Визначена мета обумовлює наступні завдання:

1. Провести аналіз протоколу LLMNR та його ролі в Windows-інфраструктурі;
2. Дослідити механізми експлуатації LLMNR-вразливостей та їх потенційні наслідки;
3. Здійснити оцінку ризиків та розробити модель загроз для корпоративної мережі;

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Спроектувати захищену мережеву архітектуру з функціональною сегментацією;
5. Реалізувати систему моніторингу на базі технології RSPAN та засобів контролю доступу;
6. Провести тестування розробленої підсистеми в емуляційному середовищі GNS3;
7. Оцінити ефективність запропонованих захисних заходів та їх практичну застосовність.

Об'єкт дослідження – процеси функціонування протоколу LLMNR у корпоративних Windows-мережах та пов'язані з ними вразливості безпеки.

Предмет дослідження – методи та технології захисту від LLMNR-атак через мережеву сегментацію, моніторинг трафіку та контроль доступу в корпоративних інфраструктурах.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної корпоративної мережі з інтегрованими засобами виявлення та протидії LLMNR-атакам, що реалізує практичні механізми мінімізації ризиків компрометації Windows-інфраструктури через експлуатацію вразливостей протоколів розв'язання імен.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. АНАЛІЗ ПРОТОКОЛУ LLMNR, ЙОГО ЗАСТОСУВАНЬ В КОРПОРАТИВНІЙ ІНФРАСТРУКТУРІ ТА НЕДОЛІКІВ БЕЗПЕКИ

1.1. Принципи роботи служб розв'язання імен у Windows-середовищі

Розв'язання імен є функцією перетворення мережевого імені на одну або кілька IP-адрес. У Windows-системах підтримується розв'язання як повністю кваліфікованих доменних імен DNS (FQDN), так і однослівних імен. Однослівні імена можуть розв'язуватися як DNS-імена та NetBIOS-імена. Для того щоб однослівне ім'я було розв'язане через DNS, воно має бути перетворене на FQDN шляхом додавання суфіксів (наприклад, "bordiuh" перетворюється на "bordiuh.ztu.com") [8].

DNS (Domain Name System) визначений у стандартах RFC1034 та RFC1035, є розподіленою системою резолверів імен. DNS-імена представляють собою повністю кваліфіковані доменні імена, такі як www.contoso.com. Результатом DNS-запиту може бути список IPv4 та IPv6 адрес, що забезпечує гнучкість у сучасних мережесередовищах з підтримкою обох версій інтернет-протоколу.

NetBIOS-розв'язання імен, стандартизоване в RFC1001 та RFC1002, перетворює NetBIOS-ім'я на одну або більше IPv4-адрес. NetBIOS-ім'я являє собою 16-байтний рядок, що активно використовується службою "Доступ до файлів та принтерів для мереж Microsoft" на комп'ютерах Windows. При запуску Windows-комп'ютера служба файлів та принтерів реєструє унікальне NetBIOS-ім'я, засноване на імені комп'ютера. Конкретне NetBIOS-ім'я формується шляхом доповнення імені комп'ютера до 15 байтів та додавання 16-го байта зі значенням 0x20, що вказує на зв'язок імені зі службою файлів та принтерів.

Типовим прикладом NetBIOS-розв'язання є перетворення імені Windows-домену на список IP-адрес контролерів домену. NetBIOS-ім'я для Windows-домену формується шляхом доповнення доменного імені до 15 байтів пробілами та додавання байта 0x01, що позначає службу контролера домену.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Windows Internet Name Service (WINS) є реалізацією Microsoft для NetBIOS Name Server (NBNS) – сервера імен для NetBIOS-імен, що забезпечує централізоване управління та реплікацію NetBIOS-записів.

Link-Local Multicast Name Resolution (LLMNR) являє собою специфікований у RFC4795, забезпечує розв'язання імен у сценаріях, коли традиційне DNS-розв'язання неможливе в локальному мережевому сегменті. Профіль LLMNR у Windows відрізняється від стандарту тим, що підтримка TCP та EDNS0, обов'язкова у RFC4795, є опціональною у Windows-реалізації. Протокол розв'язання однорангових імен (Peer Name Resolution Protocol (PNRP)) розв'язує peer-імена у набір інформації, включаючи IPv6-адреси. PNRP пропонує значні переваги над DNS завдяки своїй розподіленій природі, що робить його практично безсерверним (за винятком початкового завантаження), здатним масштабуватися до мільйонів імен та стійким до відмов.

Протокол включає безпечні служби публікації імен, дозволяючи виконувати зміни записів з будь-якої системи, на відміну від DNS, що зазвичай вимагає звернення до адміністратора DNS-сервера. Оновлення PNRP-імен відбуваються в реальному часі, що робить його придатним для високомобільних пристроїв, тоді як DNS кешує результати. Протокол виявлення мережевої інформації серверів (Server Network Information Discovery Protocol) визначає пару повідомлень запиту та відповіді, за допомогою яких клієнт може знаходити сервери протоколу в межах broadcast/multicast області та отримувати мережеву інформацію серверів, включаючи NetBIOS-імена, IPv4 та IPv6 адреси.

Багатоаспектна система розв'язання імен у Windows забезпечує надійність та гнучкість мережевої взаємодії в різних сценаріях використання, від локальних мереж до розподілених корпоративних інфраструктур.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

1.2 Протокол LLMNR

Link-Local Multicast Name Resolution (LLMNR) – це мережевий протокол, заснований на форматі пакетів системи доменних імен (DNS), який дозволяє хостам IPv4 та IPv6 виконувати розв'язання імен для інших пристроїв у межах одного локального мережевого сегменту. Протокол був вперше впроваджений у Windows Vista та Windows Server 2008, а згодом отримав підтримку в усіх наступних версіях операційних систем Microsoft, включаючи Windows 7, Windows 8, Windows 10 та відповідні серверні платформи. Окрім екосистеми Windows, LLMNR також реалізований у системі systemd-resolved на платформах Linux, що розширює його застосування в гетерогенних мережевих середовищах [12].

Технічна специфікація протоколу визначена в документі RFC 4795, проте, незважаючи на детальну розробку, LLMNR не був прийнятий як офіційний стандарт Інженерної групи Інтернету (IETF). Це пов'язано з певними обмеженнями та потенційними проблемами безпеки, які були виявлені під час розгляду протоколу. Варто зазначити, що станом на квітень 2022 року компанія Microsoft розпочала процес поступового відмовлення від використання як LLMNR, так і системи розв'язання імен NetBIOS на користь більш сучасного та безпечного протоколу Multicast DNS (mDNS). Ця зміна стратегії відображає еволюцію підходів до мережевої безпеки та прагнення до стандартизації протоколів розв'язання імен у локальних мережах. Формат заголовка LLMNR представлено на рис.1.1.

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	ID															
16	QR	Opcode				C	TC	T	Z	Z	Z	Z	RCODE			
32	QDCOUNT															
48	ANCOUNT															
64	NSCOUNT															
80	ARCOUNT															

Рисунок 1.1 – Вигляд заголовку пакету

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Протокол Link-Local Multicast Name Resolution використовує формат заголовка DNS, визначений у специфікації RFC 1035, з певними винятками та модифікаціями, що адаптують його до специфіки локальної мережевої взаємодії. Структура заголовка LLMNR є ідентичною до стандартного DNS-заголовка за розміром та загальною організацією, проте має суттєві відмінності в інтерпретації та використанні окремих полів.

Центральним елементом заголовка є поле ідентифікатора (ID), що займає 16 біт і присвоюється програмою, яка генерує запит будь-якого типу. Цей ідентифікатор відіграє критичну роль у забезпеченні надійності комунікації, оскільки копіюється з запиту до відповіді та дозволяє відправнику ефективно зіставляти отримані відповіді з активними запитами. Особливістю LLMNR є вимога встановлення псевдовипадкового значення поля ID у запиті, що підвищує безпеку протоколу та зменшує ймовірність конфліктів при одночасному функціонуванні множинних застосунків.

Поле Query/Response (QR) займає лише один біт, але має фундаментальне значення для розрізнення типу повідомлення. Коли цей біт встановлений, повідомлення інтерпретується як LLMNR-відповідь, а коли скинутий – як LLMNR-запит. Ця бінарна логіка забезпечує чітке розмежування між ініціацією запиту та наданням відповіді в рамках протоколу.

Код операції (OPCODE) представлений 4-бітовим полем, що специфікує конкретний тип запиту в повідомленні. Значення цього поля встановлюється ініціатором запиту та незмінно копіюється у відповідь, забезпечуючи цілісність контексту взаємодії. Поточна специфікація LLMNR визначає поведінку виключно для стандартних запитів та відповідей з значенням opcode рівним нулю, залишаючи можливість для майбутніх розширень протоколу.

Особливого значення набуває поле конфлікту (C), що реалізує механізм виявлення та обробки ситуацій множинних відповідей. При встановленні цього біта в запиті сигналізується про те, що відправник вже отримав декілька LLMNR-відповідей на даний запит, що може свідчити про конфлікт імен в локальній мережі.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

У контексті відповіді цей біт вказує на унікальність або неунікальність імені: якщо ім'я вважається унікальним, біт С залишається скинутим, інакше встановлюється.

Механізм обрізання повідомлень реалізується через поле TC (TrunCation), що вказує на ситуацію, коли повідомлення було скорочено через перевищення максимально дозволеної довжини для каналу передачі. Критично важливою особливістю LLMNR є заборона встановлення біта TC у запитах, а у випадку його наявності – повне ігнорування респондером. Коли біт TC встановлений у відповіді, це сигналізує відправнику про необхідність повторного надсилання запиту через TCP-протокол з використанням unicast-адреси респондера.

Поле Tentative (T) реалізує складний механізм верифікації унікальності імен у локальній мережі. Цей біт встановлюється у відповіді, коли респондер є авторитетним для певного імені, проте ще не завершив процес перевірки його унікальності. Така ситуація може виникати під час ініціалізації мережеслужб або при динамічній реконфігурації мережі. Респондер зобов'язаний ігнорувати біт T у вхідних запитах, незалежно від його стану.

Чотири біти заголовка зарезервовані для майбутнього використання (поля Z) та повинні встановлюватися в нульове значення як у запитах, так і у відповідях згідно з поточною специфікацією. Реалізації протоколу зобов'язані ігнорувати ці біти, якщо вони встановлені у вхідних повідомленнях, що забезпечує зворотну сумісність з майбутніми версіями стандарту.

Завершує структуру заголовка поле коду відповіді (RCODE), що займає 4 біти та встановлюється виключно у LLMNR-відповідях. У запитах відправник зобов'язаний встановлювати RCODE у нульове значення, яке респондер ігнорує та інтерпретує як нуль. Специфікою LLMNR є вимога встановлення нульового RCODE у відповідях на multicast-запити, що відрізняє його від поведінки традиційного DNS.

Структура лічильників секцій повідомлення. Архітектура LLMNR-повідомлення включає систему чотирьох 16-бітових лічильників, що забезпечують точну ідентифікацію кількості записів у відповідних секціях пакету. Лічильник QDCOUNT визначає кількість записів у секції питань та має критичну особливість

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

для LLMNR – його значення завжди повинно дорівнювати одиниці. Ця вимога відображає фундаментальний принцип протоколу: один LLMNR-запит може містити лише одне питання, що спрощує обробку та зменшує навантаження на мережеву інфраструктуру. Респондери зобов'язані відкидати запити з QDCOUNT, що не дорівнює одиниці, не надаючи жодної відповіді.

Лічильник ANCOUNT відображає кількість ресурсних записів у секції відповідей та може мати різні значення залежно від кількості записів, які респондер може надати у відповідь на конкретний запит. Для запитів значення ANCOUNT завжди повинно бути нульовим, і респондери зобов'язані відкидати запити з ненульовим значенням цього поля.

Лічильник NSCOUNT вказує на кількість ресурсних записів серверів імен у секції авторитету та також повинен мати нульове значення у LLMNR-запитах. Обробка секції авторитету у LLMNR має специфічні особливості, що відрізняють її від традиційного DNS, оскільки концепція авторитетності у локальних мережах інтерпретується по-іншому.

Четвертий лічильник ARCOUNT визначає кількість ресурсних записів у секції додаткових записів. Ця секція може містити супутню інформацію, що не є прямою відповіддю на запит, але може бути корисною для оптимізації подальших запитів або надання контекстної інформації.

Алгоритми поведінки відправника. Механізм функціонування відправника в протоколі LLMNR характеризується високою гнучкістю та адаптивністю до умов локальної мережі. Відправник має можливість ініціювати LLMNR-запит для практично будь-якого допустимого типу ресурсного запису, включаючи записи типу A для IPv4-адрес, AAAA для IPv6-адрес, PTR для зворотного розв'язання імен, SRV для сервісних записів, та інші типи згідно зі стандартами DNS. Ці запити направляються на спеціальну multicast-адресу локального сегмента, що забезпечує доставку повідомлення всім потенційним респондерам у межах поточного мережевого сегмента.

Критично важливою особливістю роботи відправника є необхідність готовності до ситуацій повної відсутності відповідей на LLMNR-запити. Така

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

ситуація може виникати з різних причин: відсутність респондерів у локальному сегменті, мережеві збої, або просто відсутність запитуваного ресурсу. У таких випадках розв'язувач імен інтерпретує відсутність відповіді як індикацію того, що запитуване ім'я не існує в локальному контексті, що еквівалентно отриманню відповіді з кодом помилки RCODE=3.

Обробка дублікатних відповідей реалізується через механізм ідентифікації унікальних комбінацій IP-адреси джерела та поля ідентифікатора. Відправник зобов'язаний відкидати відповіді, що мають ідентичні значення цих параметрів з уже обробленими відповідями, що запобігає дублюванню інформації та зменшує навантаження на систему обробки.

Особливої уваги потребує обробка множинних валідних LLMNR-відповідей з встановленим бітом конфлікту. У таких ситуаціях відправник повинен об'єднати всі відповіді з встановленим бітом C та обробляти їх аналогічно до множинних ресурсних записів, отриманих від єдиного DNS-сервера. Проте критично важливо не змішувати відповіді з встановленим бітом C з відповідями, де цей біт скинутий – у таких випадках пріоритет надається відповідям з встановленим бітом конфлікту.

Архітектура функціонування LLMNR-респондера базується на принципах локальної авторитетності та ефективної unicast-комунікації. Фундаментальною вимогою є надсилання всіх LLMNR-відповідей виключно через unicast-з'єднання безпосередньо до відправника запиту, що забезпечує ефективне використання мережевих ресурсів та зменшує загальний трафік у локальному сегменті.

Процес ініціалізації респондера при конфігуруванні IP-адреси включає автоматичний синтез відповідних ресурсних записів типу A, AAAA та PTR. Цей механізм дозволяє респондеру автоматично стати авторитетним для власних мережевих ідентифікаторів без необхідності ручної конфігурації. Синтез SOA-запису відбувається лише за умови наявності додаткових ресурсних записів, оскільки SOA-запис не може бути єдиним записом, за який відповідає респондер.

Мережева взаємодія респондера регламентується суворими вимогами щодо портів та адрес. Респондер зобов'язаний здійснювати прослуховування на UDP-порті 5355 для multicast-адреси локального сегмента, а також на TCP-порті 5355

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

для unicast-адрес, які можуть використовуватися як адреси джерела при надсиланні відповідей. Направлення відповідей повинно здійснюватися точно на той порт, з якого було отримано запит, при цьому відповіді завжди надсилаються з того ж порту, на який вони були направлені [11].

Принцип авторитетності у LLMNR має кардинальні відмінності від традиційного DNS. Респондер зобов'язаний відповідати виключно на запити стосовно імен та адрес, для яких він є безпосередньо авторитетним, та категорично заборонено використовувати будь-які дані з кешу LLMNR або DNS-розв'язувача. На відміну від звичайної DNS-термінології, де сервер, авторитетний для зони, є авторитетним для всіх доменних імен під вершиною зони, LLMNR-респондер має авторитетність виключно для вершини зони.

Це обмеження авторитетності має принципове значення для запобігання конфліктам у ситуаціях співіснування декількох хостів з іменами, що представляють ієрархічні відносини в DNS-просторі імен. Наприклад, хост з іменем "foo.example.com" не може відповідати на запити стосовно "child.foo.example.com", навіть якщо логічно він міг би вважатися батьківським у ієрархії. Така поведінка запобігає виникненню неоднозначних ситуацій, коли один запит може отримати множинні авторитетні відповіді різного типу від різних респондерів.

Microsoft має власну специфікацію MS-LLMNRP, яка визначає профіль Link Local Multicast Name Resolution Protocol для використання в Windows-середовищі. Цей профіль базується на стандарті RFC 4795, але містить суттєві модифікації та спрощення, спрямовані на оптимізацію роботи в типових корпоративних мережах Microsoft [10].

Основні відмінності MS-LLMNRP від базового стандарту. Обробка повідомлень та розміри пакетів. На відміну від RFC 4795, який обмежує розмір UDP-відповідей розміром MTU або 9194 октетами, MS-LLMNRP дозволяє відправникам приймати відповіді розміром до максимального UDP payload, що може бути переданий через IPv4 або IPv6. Це значно збільшує пропускну здатність для передачі великих ресурсних записів.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Респондери в MS-LLMNRP профілі повинні відправляти UDP-відповіді розміром до максимального UDP payload. Якщо всі ресурсні записи не поміщаються в UDP-пакет, респондер повинен включити стільки записів, скільки поміщається, і відправити відповідь без встановлення TC біта, що спрощує обробку truncated повідомлень.

Спрощення TCP-обробки. Базовий стандарт RFC 4795 вимагає обов'язкового використання TCP для unicast запитів та рекомендує TCP для PTR запитів. MS-LLMNRP значно спрощує цю вимогу - респондери можуть, але не зобов'язані слухати TCP порт 5355. Замість цього профіль рекомендує використовувати UDP multicast навіть для PTR запитів, що зменшує складність імплементації.

Обробка TC біта. Коли отримується відповідь з встановленим TC бітом, RFC 4795 рекомендує відкинути відповідь та повторити запит через TCP. MS-LLMNRP змінює цю поведінку - відправник повинен просто ігнорувати TC біт та обробляти відповідь так, ніби truncation не відбулося. Це спрощує логіку обробки та зменшує навантаження на мережу.

Мінімізація затримок. RFC 4795 специфікує випадкові затримки (JITTER_INTERVAL) для запитів та відповідей з метою уникнення синхронізації. MS-LLMNRP відмовляється від цієї практики, рекомендуючи відправляти запити та відповіді негайно без випадкових затримок. Це значно покращує час відгуку системи розв'язання імен.

Підтримка інтернаціоналізації. Важливою особливістю MS-LLMNRP є чітка вимога щодо кодування імен. Відправники повинні відправляти запити в UTF-8 форматі, а не в Punycode, як це може бути в базовому стандарті. Респондери повинні відповідати на запити для імен, закодованих у UTF-8, та можуть підтримувати Punycode для інтернаціональних доменних імен.

Селективна підтримка типів записів. MS-LLMNRP профіль чітко визначає, що респондери повинні відповідати на запити для ресурсних записів типу A, AAAA, PTR та ANY. Для інших типів записів респондери можуть відповідати, але рекомендується мовчки відкидати такі запити. При запиті типу ANY респондер повинен повернути всі доступні A та AAAA записи.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Спрощення конфігурації. На відміну від базового стандарту, який припускає можливість розширюваного сховища даних для імен, MS-LLMNRP не вимагає налаштовуваного або розширюваного сховища імен. Це спрощує імплементацію для типових Windows-хостів, які зазвичай відповідають лише за власні імена.

Практичні переваги в Windows-середовищі. Ці модифікації роблять LLMNR більш ефективним у типових Windows-мережах, де швидкість розв'язання імен критична для продуктивності користувачів. Зменшення затримок, спрощення TCP-обробки та оптимізація розмірів пакетів забезпечують кращу інтеграцію з екосистемою Windows, особливо в сценаріях із великою кількістю клієнтів та інтенсивним мережевим трафіком.

Водночас, MS-LLMNRP зберігає сумісність із базовими принципами RFC 4795, дозволяючи взаємодію з іншими LLMNR-сумісними пристроями в мережі, що робить його практичним рішенням для гетерогенних мережевих середовищ.

1.3 Застосування LLMNR у корпоративній інфраструктурі

Корпоративні мережі мають відносно довгу історію, що охоплює шість десятиліть і сягає корінням до ранніх днів комп'ютерних технологій. Сьогодні наші пристрої легко перемикаються між мережами, а дані безперешкодно переміщуються по всій планеті для забезпечення оптимального шляху передачі інформації. Мережі пройшли довгий шлях від простого з'єднання двох мейнфреймів в одній будівлі за допомогою дротів до управління мільйонами пристроїв через різноманітні дротові та бездротові з'єднання [9].

Сучасна корпоративна мережева архітектура являє собою складну систему, що включає комбінацію різних технологій та протоколів для забезпечення безпечної та надійної інфраструктури. Основними компонентами такої архітектури є брандмауери як пристрої безпеки, що контролюють вхідний та вихідний мережевий трафік і зазвичай розміщуються на периметрі мережі для захисту від несанкціонованого доступу та кібератак. Віртуальні приватні мережі (VPN) забезпечують безпечне підключення віддалених користувачів до корпоративної мережі, використовуючи шифрування для захисту даних під час передачі через

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

інтернет. Маршрутизатори та комутатори як мережеві пристрої пересилають та фільтрують мережевий трафік, з'єднуючи різні частини мережі та контролюючи потоки даних. Точки бездротового доступу забезпечують бездротове підключення для ноутбуків, смартфонів та планшетів без необхідності використання кабелів [7].

Системи виявлення та запобігання вторгненням (IDS/IPS) моніторять мережу на предмет підозрілої активності та можуть вживати заходів для її запобігання або блокування. Балансувальники навантаження розподіляють вхідний мережевий трафік між кількома серверами, допомагаючи забезпечити доступність та відгук мережі навіть під час високого навантаження. Інтеграція з хмарою дозволяє доступ та використання хмарних ресурсів і сервісів, таких як Software as a Service (SaaS), Infrastructure as a Service (IaaS) та Platform as a Service (PaaS). Сегментація мережі як процес поділу мережі на менші, ізольовані сегменти допомагає покращити безпеку, обмежуючи поширення потенційних порушень або шкідливого програмного забезпечення. SD-WAN технологія дозволяє управління з'єднаннями глобальної мережі через програмне забезпечення, використовуючи його для динамічного контролю та оптимізації мережевого трафіку через кілька типів з'єднань.

Для управління великими корпоративними мережами зазвичай використовується прагматичний підхід з акцентом на простоту та надійність. Менеджери корпоративних мереж повинні намагатися забезпечити надійну мережу без великих вимог до людських ресурсів, тому складні системи управління мережами не є поширеною особливістю. Натомість використовується простий підхід з обґрунтуванням, що прості дизайни мають прості збої, які легко виправити. Багато корпорацій обирають використання набору простіших інструментів управління: PING для тестування доступності мережевих пристроїв, traceroute для відстеження шляху пакетів через мережу, та Multi-Router Traffic Grapher (MRTG), який використовує SNMP для читання MIB змінних та створення графіків, що представляють навантаження трафіку на мережевих лінках. MRTG генерує HTML-сторінки з GIF-зображеннями, які забезпечують живе візуальне представлення

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

трафіку, що дозволяє ефективно управляти великими національними IP-мережами разом з NetView та деякими внутрішніми інструментами [18].

Протокол LLMNR забезпечує критично важливу функціональність у корпоративних мережах завдяки можливості розв'язання імен локальних вузлів навіть за відсутності централізованого DNS-сервера. Це особливо цінно для організацій із розподіленою інфраструктурою, де окремі філії можуть тимчасово втрачати з'єднання з основними корпоративними DNS-серверами. LLMNR активується автоматично в операційних системах Windows і функціонує без додаткового адміністративного втручання, що значно знижує навантаження на IT-відділи. Протокол демонструє високу ефективність при розв'язанні імен ресурсів у межах локального мережевого сегмента, забезпечуючи швидкий доступ до файлових серверів, принтерів та інших локальних сервісів. Підтримка як IPv4, так і IPv6 протоколів дозволяє інтегрувати LLMNR в сучасні корпоративні мережі з різними технологічними рішеннями, а використання як доповнення до основної DNS-інфраструктури оптимізує витрати на мережеве обладнання.

Однак LLMNR має суттєві обмеження та ризики, які необхідно враховувати при його впровадженні. Фундаментальним обмеженням є його нездатність працювати за межами локального мережевого сегмента або широкомовного домену - протокол не може пересікати маршрутизатори або забезпечувати розв'язання імен між різними підмережами, що суттєво обмежує його застосування в складних корпоративних мережах із багаторівневою ієрархічною архітектурою. У великих корпоративних мережах із сотнями або тисячами робочих станцій LLMNR може створювати додаткове навантаження на мережевий трафік через широкомовні запити, оскільки кожен неуспішний DNS-запит призводить до генерації LLMNR-трафіку, що може негативно впливати на пропускну здатність мережі.

Хоча LLMNR технічно сумісний з IPv6, його ефективність в таких мережах значно поступається спеціалізованим протоколам, зокрема Neighbor Discovery Protocol (NDP). У корпоративних середовищах, що активно впроваджують IPv6 або використовують змішані IPv4/IPv6 конфігурації, це може створювати складнощі в

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

забезпеченні стабільного розв'язання імен. Ефективність LLMNR суттєво залежить від правильного налаштування мережевого обладнання та політик безпеки - брандмауери, системи запобігання вторгненням або неправильно налаштовані комутатори можуть блокувати або обмежувати LLMNR-трафік, що призводить до непередбачуваної поведінки системи розв'язання імен.

На відміну від традиційної DNS-інфраструктури, LLMNR не надає можливостей для централізованого управління та моніторингу. IT-адміністратори не можуть легко відстежувати або контролювати LLMNR-активність в мережі, що ускладнює діагностику проблем та планування розвитку мережевої інфраструктури. В деяких корпоративних середовищах одночасне використання LLMNR разом з іншими протоколами локального розв'язання імен (наприклад, NetBIOS або mDNS) може призводити до конфліктів або непередбачуваної поведінки мережевих сервісів, особливо при використанні різноманітного обладнання від різних виробників.

Проектування корпоративних мереж є критично важливим процесом, що потребує ретельного планування та дотримання перевірених практик. Оскільки мережі стають критично важливими для бізнес-функцій, проектні рішення, прийняті IT-професіоналами, можуть мати далекосяжні наслідки. Мережа з добре спланованим дизайном працюватиме краще, буде більш безпечною та стійкою, простішою для усунення несправностей, легко масштабуватиметься та адаптуватиметься до майбутніх технологій. Мережеві архітектори прагнуть створити надійну архітектуру, яка демонструє високу продуктивність та є доступною для побудови, експлуатації та обслуговування. Важливо розуміти, що проектування мережі охоплює бізнес-процеси та результати, тоді як мережева топологія відноситься до дизайну, який розглядається через мережеві діаграми, часто називані топологічними картами [23].

Мережева діаграма зазвичай є основним інструментом процесу проектування, забезпечуючи візуальне представлення мережі та інтегруючи інформацію про фізичні з'єднання, кількість, тип та розташування всіх пристроїв та кінцевих точок, IP-адресацію, процеси безпеки та архітектуру. При побудові

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

мережі з нуля першим кроком є складання списку всіх активів, кінцевих точок, користувачів, пристроїв, локальних мереж та інших мережевих елементів. При проектуванні для існуючих мережевих середовищ процес інтегрує наявну інфраструктуру, яка повинна підтримуватися або продовжувати працювати під час виробництва та розгортання нової мережі.

Успішне проектування базується на фундаментальних принципах, які забезпечують створення інфраструктури, здатної підтримувати потреби підприємства. Визнання цінності дизайну є першочерговим - проектування мереж, які виконують критичні бізнес-функції, повинно бути ретельно продуманим процесом. Гнучкість та масштабованість є основоположними, оскільки підприємства розвиваються і їхні мережеві потреби змінюються. Корпоративна мережа повинна мати здатність адаптуватися до цих змін, а можливість масштабування в різних частинах мережі для задоволення попиту є одним з найважливіших аспектів мережевої гнучкості.

Резервування додає додаткову ємність в мережі шляхом формування множинних з'єднань між компонентами та створення кількох шляхів від одного компонента до іншого. Коли шлях переривається або компонент стає недоступним, протоколи відмовостійкості допомагають решті частин з'ясувати, як спілкуватися один з одним через альтернативний шлях. Проектування для стійкості починається зі створення списку викликів стійкості, з якими стикається організація - таких як інциденти безпеки, мережеві проблеми або раптова потреба в оновленні додатків чи масштабуванні. Проектування для видимості включає впровадження системи управління мережею (NMS), яка може допомогти забезпечити видимість мережі, полегшуючи ІТ-командам виявлення потенційних проблем та моніторинг показників продуктивності.

Ключовими практиками проектування є інтеграція безпеки з самого початку - безпека мережі повинна бути вбудована на ранніх стадіях проектування, а не додаватися пізніше. Якщо безпека не враховується в дизайні, несумісні інструменти безпеки можуть вплинути на продуктивність мережі, користувацький досвід та керованість. Концепція "зміщення безпеки вліво" зменшує ймовірність

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

прогалин у безпековій позиції та підвищує загальну продуктивність мережі. Важливо розуміти коли використовувати підходи "зверху вниз" проти "знизу вгору" - у більшості випадків при початку з нуля проектування "зверху вниз" є кращим вибором, оскільки зосереджується на бізнес-вимогах та максимізує шанси на успіх [2].

Стандартизація всіх можливих елементів значно полегшує усунення несправностей, встановлення патчів, обслуговування та управління активами в довгостроковій перспективі. Це включає імена хостів, моделі обладнання, схеми IP-адресації, кольори кабелів та політики безпеки. Планування зростання є критичним, оскільки споживання мережевої пропускної здатності сьогодні не буде таким же через рік. Необхідно врахувати, наскільки очікується збільшення споживання пропускної здатності протягом життєвого циклу мережі, та проектувати з урахуванням цих очікувань. Забезпечення того, щоб мережа була достатньо гнучкою та модульною для легкого розширення, можливо, ще важливіше.

Постійне проектування у відповідь на еволюцію мережевих потреб є необхідним, оскільки у міру зростання та зміни бізнесу його мережа також повинна змінюватися. Користувачі та клієнти приходять і йдуть, додатки розвиваються, а робочі звички змінюються. Високопродуктивний, економічно ефективний мережевий дизайн потребує коригування для врахування цих змін. Проектування для сталого розвитку може включати впровадження системи глобального управління енергією, ініціативи зі зниження викидів парникових газів та впровадження енергетичних функцій для зменшення глобального попиту на енергію [1].

Висновки до першого розділу

Проведений аналіз служб розв'язання імен у Windows-середовищі та детальне дослідження протоколу LLMNR дозволяють зробити наступні висновки:

Сучасна екосистема розв'язання імен у Windows представляє собою багаторівневу архітектуру, що включає традиційні DNS-сервіси, спадкові NetBIOS-

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

механізми та інноваційні локальні протоколи, серед яких LLMNR займає особливе місце як перехідне рішення між класичними та сучасними підходами до мережевої ідентифікації.

Протокол LLMNR демонструє значні технічні переваги в контексті локального розв'язання імен, забезпечуючи автономність мережевих сегментів від централізованої DNS-інфраструктури та підтримуючи безперервність сервісів навіть при втраті зв'язку з основними серверами імен. Особливо цінною є його здатність функціонувати без додаткового адміністративного втручання та автоматична інтеграція з існуючими Windows-системами.

Модифікації Microsoft у специфікації MS-LLMNRP свідчать про прагматичний підхід компанії до оптимізації протоколу для корпоративного використання. Спрощення TCP-обробки, мінімізація затримок та оптимізація розмірів пакетів роблять LLMNR більш ефективним у типових Windows-мережах, водночас зберігаючи базову сумісність зі стандартом RFC 4795.

Однак аналіз виявив суттєві обмеження протоколу, які обмежують його застосування в складних корпоративних інфраструктурах. Неможливість пересікання маршрутизаторів, потенційне збільшення мережевого трафіку через широкомовні запити та відсутність централізованого управління створюють серйозні виклики для великих розподілених мереж.

Особливо важливим є розуміння того, що LLMNR слід розглядати не як заміну традиційного DNS, а як доповнюючий механізм для специфічних сценаріїв використання. Його найбільша цінність проявляється в малих та середніх мережевих сегментах, де необхідна швидка та надійна локальна ідентифікація ресурсів.

Еволюція підходу Microsoft до відмови від LLMNR на користь mDNS відображає загальну тенденцію галузі до стандартизації протоколів розв'язання імен. Це рішення підкреслює важливість довгострокового планування мережевої архітектури та необхідність врахування майбутніх технологічних трендів при проектуванні корпоративних інфраструктур.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Результати дослідження вказують на те, що успішне впровадження LLMNR вимагає ретельного аналізу специфічних потреб організації, архітектури мережі та довгострокової стратегії розвитку ІТ-інфраструктури. Протокол може забезпечити значну користь у відповідних умовах, але його обмеження необхідно враховувати на етапі планування для уникнення майбутніх проблем масштабування та інтеграції.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

РОЗДІЛ 2 ПРОЕКТУВАННЯ ПІДСИСТЕМИ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЛАНУВАННЯ ЗАХОДІВ БЕЗПЕКИ

2.1 Механізми експлуатації та сценарії LLMNR-атак

Зловмисник, який отримав доступ до локальної мережі, використовує спеціалізовані інструменти, такі як Responder, для прослуховування LLMNR-запитів. Коли користувач або система намагається отримати доступ до ресурсу, який не може бути розв'язаний через DNS, генерується LLMNR-запит. Атакуючий перехоплює цей запит та надає фальшиву відповідь, вказуючи власну IP-адресу як адресу запитуваного ресурсу. Коли жертва намагається автентифікуватися на підроблений сервер, її облікові дані (зокрема, Net-NTLMv2 хеші) передаються атакуючому. Ці хеші можуть бути використані для атак offline brute-force або pass-the-hash атак [13].

На основі цих базових механізмів експлуатації LLMNR можуть бути реалізовані різноманітні сценарії атак, які можуть мати катастрофічні наслідки для корпоративної інфраструктури. Найбільш критичним є сценарій компрометації контролера домену, який розгортається після успішного отримання облікових даних привілейованих користувачів. Використовуючи захоплені облікові дані, зловмисник може отримати доступ до контролера домену - центрального компонента інфраструктури Active Directory. Після компрометації контролера домену атакуючий отримує можливість модифікувати об'єкти AD, створювати нові облікові записи, змінювати налаштування безпеки та здійснювати інші дії, що можуть призвести до повної компрометації домену. Цей сценарій є критично небезпечним, оскільки контролер домену містить всю інформацію про користувачів, групи, політики безпеки та інші важливі компоненти корпоративної інфраструктури.

Не менш небезпечним є сценарій латерального переміщення в мережі, який дозволяє атакуючому розширити свій вплив після початкової компрометації. Використовуючи отримані через LLMNR poisoning облікові дані, зловмисник може переміщуватися між різними системами в мережі, поступово розширюючи свій

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

доступ та привілеї. Цей процес може включати компрометацію додаткових робочих станцій, серверів та сервісів, що дозволяє атакуючому отримати доступ до більш цінних ресурсів та інформації.

Особливу увагу заслуговує сценарій зловживання довірчими відносинами, який використовує специфіку архітектури Active Directory, де домени можуть мати довірчі відносини між собою. Експлуатуючи LLMNR, атакуючий може маніпулювати цими довірчими відносинами для переміщення між доменами. Це дозволяє зловмиснику потенційно отримати доступ до ресурсів в інших частинах організації, включаючи дочірні компанії або філії, які мають довірчі відносини з компрометованим доменом.

В сучасних умовах все більшої актуальності набуває сценарій атаки на бездротові мережі, особливо в контексті публічних точок доступу та корпоративних Wi-Fi мереж. У таких середовищах атакуючий може фізично знаходитися на значній відстані від цілі, але все ще мати доступ до локальної мережі. Відсутність належного захисту на каналному рівні (наприклад, IEEE 802.11i) робить такі мережі особливо вразливими до LLMNR-атак. Зловмисник може створити підроблену точку доступу або підключитися до існуючої мережі та здійснювати атаки poisoning на всіх підключених пристроїв [17].

Найскладнішим для виявлення та протидії є сценарій комбінованої атаки, який передбачає використання LLMNR poisoning в поєднанні з іншими техніками кібератак. Наприклад, атакуючий може спочатку здійснити атаку на DNS-сервери, щоб змусити системи переключитися на LLMNR, а потім використовувати poisoning для отримання облікових даних. Альтернативно, LLMNR може використовуватися як допоміжний інструмент в рамках більш складних атак, таких як Advanced Persistent Threats (APT), де основна мета полягає в довгостроковому прихованому доступі до корпоративної мережі.

2.2 Оцінка ризиків для корпоративної інфраструктури

Оцінка ризиків, пов'язаних з експлуатацією вразливостей протоколу LLMNR, є критично важливою для розуміння потенційного впливу на корпоративну

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

інфраструктуру. Комплексний аналіз ризиків повинен враховувати як технічні аспекти вразливостей, так і бізнес-процеси організації, що можуть постраждати від успішних атак.

Ризик компрометації облікових даних оцінюється як високий, оскільки LLMNR poisoning атаки дозволяють зловмисникам отримувати Net-NTLMv2 хеші без складних технічних маніпуляцій. Ймовірність успіху таких атак є високою в середовищах, де LLMNR активний за замовчуванням, особливо в мережах з великою кількістю користувачів, які регулярно звертаються до мережевих ресурсів. Потенційний вплив включає не лише компрометацію окремих облікових записів, але й можливість використання цих облікових даних для ескалації привілеїв та доступу до критично важливих систем. Фінансові наслідки можуть бути значними, включаючи витрати на розслідування інциденту, відновлення систем, можливі штрафи за порушення конфіденційності даних та втрату репутації [19].

Ще більш серйозним є ризик повної компрометації домену Active Directory, який є критичним для більшості корпоративних організацій. Якщо атакуючий отримує доступ до контролера домену через LLMNR-атаку, наслідки можуть бути катастрофічними. Цей ризик включає можливість модифікації політик безпеки, створення backdoor-ів, крадіжки чутливих даних та повного порушення роботи IT-інфраструктури. Ймовірність реалізації цього ризику залежить від архітектури мережі, наявності належного сегментування та рівня привілеїв користувачів, облікові дані яких можуть бути скомпрометовані. Відновлення після такого інциденту може вимагати повної перебудови домену, що призводить до значних простоїв та фінансових втрат.

Довгострокові загрози для організації створює ризик латерального переміщення в мережі. Атакуючі, які успішно експлуатують LLMNR, можуть поступово розширювати свій доступ, залишаючись непоміченими протягом тривалого періоду. Цей ризик особливо актуальний для організацій з великими та складними мережевими інфраструктурами, де виявлення несанкціонованої активності може бути ускладнено. Довгострокове присутність зловмисників в

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

мережі може призвести до промислового шпигунства, крадіжки інтелектуальної власності та поступової компрометації всіх критично важливих систем.

Значну увагу заслуговує ризик порушення нормативних вимог, особливо для організацій, які підлягають регулюванню у сферах захисту персональних даних (GDPR, CCPA), фінансових послуг (PCI DSS) або охорони здоров'я (HIPAA). LLMNR-атаки можуть призвести до несанкціонованого доступу до конфіденційних даних, що може спричинити порушення нормативних вимог. Потенційні наслідки включають значні штрафи, обов'язкові повідомлення про порушення, додаткові аудити та можливі судові позови. Репутаційні ризики також можуть мати довгостроковий вплив на бізнес-операції організації.

Безпосередньо на бізнес-процеси впливає ризик операційних збоїв, пов'язаний з потенційними порушеннями в роботі критично важливих систем. LLMNR-атаки можуть призвести до недоступності ключових систем, порушення комунікацій між додатками та сервісами, а також до необхідності екстрених заходів щодо відновлення. Для організацій, які залежать від безперервної роботи ІТ-систем, такі збої можуть призвести до значних фінансових втрат, порушення договірних зобов'язань та втрати клієнтів.

Особливо складним є ризик розповсюдження атаки на партнерські організації, актуальний для компаній, які мають довірчі відносини з іншими організаціями через VPN-з'єднання або федерації. Компрометація через LLMNR може потенційно поширитися на партнерські мережі, створюючи каскадний ефект та ускладнюючи процес локалізації та відновлення. Це може призвести до правових проблем, розірвання партнерських відносин та додаткових фінансових зобов'язань.

Для ефективного управління усіма зазначеними ризиками організації повинні реалізувати комплексний підхід, що включає технічні заходи (відключення LLMNR, сегментація мережі, моніторинг), організаційні процедури (навчання персоналу, процедури реагування на інциденти) та регулярні аудити безпеки для оцінки ефективності захисних заходів [21].

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

2.3 Розробка архітектури захищеної підсистеми мережі

Сегментація мережі є фундаментальним принципом проектування безпечної мережевої інфраструктури, що передбачає поділ великої мережі на менші, керовані сегменти з метою підвищення безпеки, продуктивності та спрощення управління. У контексті захисту від атак на протокол LLNMR сегментація набуває особливого значення, оскільки дозволяє обмежити поширення multicast-трафіку та локалізувати потенційні загрози в межах окремих мережевих сегментів.

Концепція мережевої сегментації виникла як відповідь на потребу в обмеженні широкомовних доменів (broadcast domains) в ранніх Ethernet-мережах, які функціонували на швидкості 10 Мбіт/с та використовували концентратори (10BaseT) або спільні магістральні з'єднання (10Base2). Первинна сегментація здійснювалася на третьому рівні моделі OSI (мережевому рівні) за допомогою маршрутизаторів, багаторівневих комутаторів та міжмережевих екранів, які блокували широкомовний трафік та дозволяли розділити велику плоску Ethernet-мережу на дискретні сегменти з меншою кількістю вузлів та, відповідно, меншою кількістю широкомовних повідомлень і меншою конкуренцією за доступ до середовища передачі [22].

З розвитком технології комутованого Ethernet та збільшенням обчислювальних можливостей мережевого обладнання з'явилася альтернативна методологія сегментації на другому рівні OSI з використанням віртуальних локальних мереж (VLAN). Технологія VLAN використовує теги в заголовку Ethernet-кадру для встановлення ідентифікатора VLAN (802.1Q), що дозволяє сумісним Ethernet-комутаторам пересилати або блокувати трафік (включаючи широкомовні повідомлення) на основі тегу 802.1Q або ідентифікатора VLAN порту (PVID). Для забезпечення зв'язку між VLAN трафік повинен бути явно маршрутизований на третьому рівні за допомогою маршрутизувального пристрою.

Сучасна мережева сегментація базується на декількох фундаментальних принципах, які забезпечують ефективний контроль трафіку та підвищення рівня безпеки. Принцип мінімізації широкомовних доменів передбачає створення окремих сегментів, в межах яких обмежується поширення широкомовного та

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

multicast-трафіку. Це особливо важливо для протоколів типу LLMNR, які використовують multicast-адресу для розсилання запитів усім хостам у локальній мережі.

Принцип контрольованого міжсегментного обміну забезпечує, що весь трафік між сегментами проходить через спеціально визначені точки контролю (choke points), де може бути здійснена інспекція, фільтрація та контроль. Такими точками можуть бути маршрутизатори, міжмережеві екрани, проксі-сервери або спеціалізовані засоби контролю доступу до мережі. Цей принцип дозволяє реалізувати детальні політики безпеки та забезпечити моніторинг міжсегментного трафіку [14].

Принцип функціональної сегментації передбачає групування мережевих ресурсів відповідно до їх функціонального призначення, рівня критичності та вимог безпеки. Наприклад, сервери баз даних, веб-сервери, робочі станції користувачів та мережеве обладнання повинні розміщуватися в окремих сегментах з відповідними політиками доступу.

У контексті промислових мереж концепція сегментації набуває додаткових вимірів через впровадження зональної сегментації. Зональна сегментація передбачає поділ промислових систем на групи підсистем з метою зменшення поверхні атаки та мінімізації векторів атак. Це досягається шляхом обмеження непотрібного потоку даних між зонами та створення чітких меж безпеки між різними функціональними областями.

Кожна зона, залежно від своєї функції, пропускної здатності, постачальника системи та власника/оператора, має власні топології, вимоги до продуктивності, потреби віддаленого доступу та мережеві сервіси. Ці фактори повинні враховуватися при проектуванні безпечної архітектури, що робить зональну сегментацію одним з найважливіших елементів кібербезпеки промислових систем.

Регулярний аудит конфігурацій сегментації та перевірка ефективності реалізованих заходів безпеки є необхідними для підтримання високого рівня захисту. Це включає перевірку налаштувань VLAN, ACL, політик multicast-

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

фільтрації та відповідності реальної топології мережі задокументованим схемам сегментації [15].

Сегментація мережі є критично важливим підходом до покращення безпеки та продуктивності корпоративних мереж. Існують два основні типи сегментації: фізична та віртуальна. Фізична сегментація передбачає розподіл різних груп пристроїв на окремі комутатори, що забезпечує найвищий рівень безпеки, але є складною у впровадженні через необхідність окремих інтернет-з'єднань, фізичного кабелювання та брандмауерів для кожної секції. Водночас, віртуальна або логічна сегментація дозволяє розділити одну фізичну мережу на кілька віртуальних сегментів за допомогою технологій як VLAN, що є більш гнучким рішенням.

Основні переваги сегментації включають посилену безпеку шляхом обмеження поширення порушень, покращену продуктивність через зменшення broadcast-трафіку та спрощення управління мережею. Адміністратори можуть швидше ідентифікувати проблеми в логічно розділених секціях, що полегшує технічне обслуговування та оновлення. Крім того, сегментація дозволяє реалізувати більш ефективні політики безпеки та контролю доступу, особливо для чутливих ресурсів, що важливо для дотримання галузевих регламентів. Масштабованість також є ключовою перевагою - додавання нових сегментів набагато простіше, ніж розширення однієї великої мережі, що робить цей підхід адаптивним до зростання організації.

Для даної мережі було обрано фізичну сегментацію. Розроблено типову корпоративну мережеву архітектуру з функціональною сегментацією, де кожен підрозділ організації отримує власний мережевий сегмент з відповідною підмережею. Структура характеризується централізованим підходом до управління трафіком через основний маршрутизатор, який координує взаємодію між сегментами відділу продажів, бухгалтерії та HR-департаменту. Кожен відділ функціонує в межах власної ізольованої підмережі, що забезпечує додатковий рівень безпеки та контролю трафіку.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Рішення включає логічне відокремлення серверних ресурсів від користувацьких робочих станцій, що відповідає сучасним принципам інформаційної безпеки, рис.2.1.

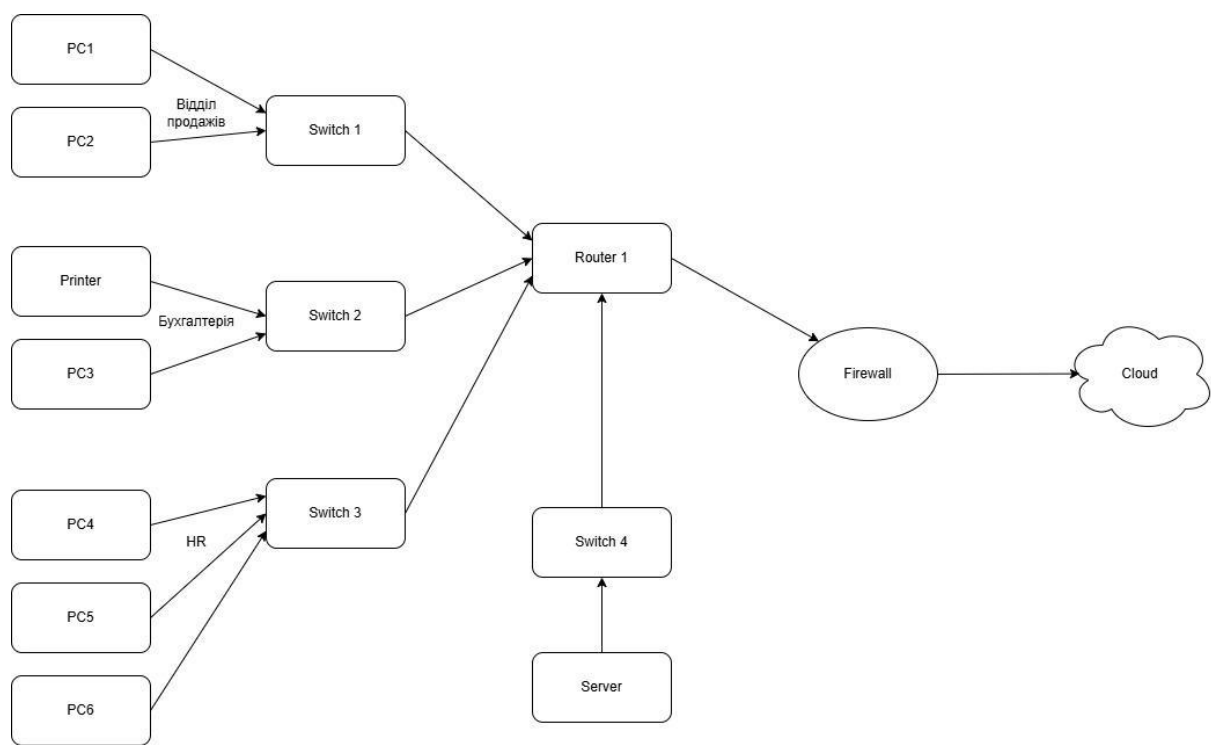


Рисунок 2.1 – Топологія мережі

Периметровий захист реалізується через брандмауер, розташований між внутрішньою інфраструктурою та зовнішнім хмарним середовищем. Така топологія з окремими підмережами для кожного відділу забезпечує базовий рівень ізоляції трафіку та дозволяє застосовувати різні політики безпеки для різних організаційних підрозділів, відповідно до вимог безпеки різних відділів.

Впровадження ефективної системи контролю доступу та моніторингу мережевої безпеки є критично важливим для захисту організаційних ресурсів від сучасних кіберзагроз. Враховуючи зростаючу складність ІТ-інфраструктури, поширення хмарних технологій та віддаленої роботи, організації потребують комплексного підходу до забезпечення безпеки доступу до своїх цифрових активів.

Контроль доступу є ключовим компонентом інформаційної безпеки, що регулює хто або що може переглядати, використовувати або отримувати доступ до певного ресурсу в обчислювальному середовищі. Основна мета полягає в

мінімізації ризиків безпеки шляхом забезпечення того, щоб лише авторизовані користувачі, системи або сервіси мали доступ до необхідних їм ресурсів.

П'ять ключових компонентів контролю доступу включають аутентифікацію як перший крок у контролі доступу, що передбачає перевірку особи користувача або системи, що запитує доступ. Це зазвичай здійснюється шляхом співставлення наданих облікових даних із збереженою інформацією. Методи аутентифікації включають парольну аутентифікацію, біометричну аутентифікацію та сертифікатну аутентифікацію [16].

Авторизація відбувається після успішної аутентифікації та передбачає надання або відмову в доступі на основі привілеїв користувача або системи. Привілеї визначаються заздалегідь і диктують, до яких ресурсів користувач або система можуть отримати доступ і в якому обсязі.

Доступ являє собою фактичне використання або взаємодію з ресурсом, що може включати перегляд, модифікацію або видалення даних, або користування сервісом. Обсяг доступу визначається процесом авторизації. Управління включає підтримку та оновлення системи контролю доступу, визначення та оновлення політик доступу, управління обліковими записами користувачів, процеси адаптації та звільнення співробітників.

Аудит передбачає моніторинг та запис шаблонів доступу і діяльності, що допомагає виявляти незвичайну або підозрілу активність і сприяє проведенню криміналістичних розслідувань. Мережевий моніторинг безпеки (NSM) збирає та аналізує дані для виявлення та реагування на загрози безпеки в мережі. Цей процес передбачає використання програмного забезпечення для моніторингу та інших технологій для отримання інформації про потік трафіку та інші важливі показники продуктивності мережі.

Ключові компоненти NSM включають визначення даних, які потребують захисту. Враховуючи обмеження часу, ресурсів та бюджету, пріоритизація є життєво важливою. Ключові дані та інфраструктура повинні мати відповідні заходи безпеки та програмне забезпечення для моніторингу. Встановлення плану виправлення недоліків безпеки необхідне, оскільки безперервний мережевий

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

моніторинг безпеки потребує доповнення іншими заходами та практиками безпеки. Потенційні слабкі місця повинні ретельно відстежуватися по всій мережі.

Підтримка постійного нагляду за кінцевими точками важлива, адже сучасні організації прийняли налаштування, сприятливі для віддаленої роботи, тому багато кінцевих точок можуть підключатися до внутрішніх мереж і потребують ретельного моніторингу. Розпізнавання аномальної поведінки користувачів можливе завдяки тому, що безперервний мережевий моніторинг безпеки надає багато інформації про поведінку користувачів, допомагаючи встановити типові шаблони користувачів у організації.

Проведення моніторингу третіх сторін також є важливим аспектом безпеки, адже спостереження за третіми сторонами, з якими організація тісно співпрацює, потребує особливої уваги. Системи управління ідентифікацією та доступом (IAM) відіграють ключову роль у сучасних стратегіях контролю доступу через централізацію управління ідентифікацією, що спрощує управління ідентифікаційними даними користувачів. Вони полегшують життєвий цикл управління користувачами від створення до видалення облікових записів, забезпечують передові методи аутентифікації та авторизації, включаючи багатофакторну аутентифікацію, покращують користувацький досвід через можливості єдиного входу (SSO).

Кращі практики безпеки включають впровадження багатофакторної аутентифікації, яка вимагає від користувачів надання двох або більше факторів перевірки для отримання доступу до ресурсу, додаючи додатковий рівень безпеки. Реалізація сильних парольних політик є важливою, адже сильні парольні політики повинні забезпечувати використання довгих, складних паролів та регулярну зміну паролів. Багато організацій розглядають можливість переходу на безпарольні методи аутентифікації.

Відмова від спільних облікових записів необхідна, оскільки спільні облікові записи ускладнюють відстеження активності користувачів та притягнення окремих осіб до відповідальності за свої дії. Принцип найменших привілеїв передбачає, що

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

користувачу надаються мінімальні рівні доступу, необхідні для виконання його робочих функцій, що мінімізує ризик зловмисної діяльності.

Прийняття парадигми нульової довіри означає, що модель нульової довіри працює за принципом "ніколи не довіряй, завжди перевіряй", що означає ретельну перевірку кожного запиту на доступ незалежно від його походження. Ефективне впровадження контролю доступу та моніторингу мережевої безпеки вимагає комплексного підходу, що поєднує сучасні технології, кращі практики та постійне удосконалення процесів. Організації повинні адаптуватися до мінливого ландшафту загроз, впроваджуючи рішення, що забезпечують баланс між безпекою та продуктивністю користувачів.

Практичні заходи з контролю доступу та моніторингу LLMNR трафіку включають контроль MAC-адрес як ефективний спосіб контролю доступу для стаціонарних робочих станцій, налаштування NetFlow моніторингу на центральному маршрутизаторі для відслідковування обсягу та напрямків LLMNR запитів, налаштування "дзеркалювання" трафіку на комутаторах з копіюванням трафіку і направленням його для аналізу, та систему захоплення пакетів на сервері для відслідковування трафіку в реальному часі.

Висновки до другого розділу

У даному розділі було проведено комплексне дослідження проектування підсистеми корпоративної мережі та планування заходів безпеки для протидії LLMNR-атакам. Аналіз механізмів експлуатації показав критичну важливість розуміння п'яти основних сценаріїв атак: компрометація контролера домену, латеральне переміщення в мережі, зловживання довірчими відносинами, атаки на бездротові мережі та комбіновані атаки. Кожен з цих сценаріїв представляє значну загрозу для корпоративної інфраструктури через можливість перехоплення multicast-запитів, надання фальшивих відповідей та захоплення облікових даних.

Оцінка ризиків виявила високий рівень загроз, особливо ризик компрометації облікових даних та повної компрометації домену Active Directory. LLMNR-атаки можуть призвести до каскадних ефектів, включаючи порушення нормативних

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

вимог, операційні збої та розповсюдження атак на партнерські організації. Фінансові наслідки включають значні витрати на відновлення, штрафи та втрату репутації.

Розроблена архітектура мережі базується на принципах функціональної сегментації з фізичним відокремленням підрозділів організації. Запропонована топологія забезпечує ізоляцію трафіку між відділами, що обмежує поширення multicast-трафіку та локалізує потенційні загрози в межах окремих сегментів. Впровадження ефективної системи контролю доступу включає п'ять ключових компонентів: аутентифікацію, авторизацію, контроль доступу, управління та аудит.

Практичні заходи моніторингу включають контроль MAC-адрес для стаціонарних робочих станцій, налаштування NetFlow моніторингу на центральному маршрутизаторі, дзеркалювання трафіку на комутаторах та систему захоплення пакетів для аналізу в реальному часі. Результати підтверджують необхідність комплексного підходу до захисту від LLMNR-атак, що поєднує технічні заходи, організаційні процедури та регулярні аудити ефективності захисних заходів для підтримання високого рівня інформаційної безпеки в корпоративних мережах.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

РОЗДІЛ 3. ВДОСКОНАЛЕННЯ МЕТОДІВ РОЗВІДКИ ТА ЗАХИСТУ В КОРПОРАТИВНІЙ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ CYBER KILL CHAIN

3.1 Проектування мережевої архітектури та вибір обладнання

При створенні корпоративної мережі для організації з декількома відділами важливо обрати надійне та перевірене обладнання. Сучасний ринок мережевих технологій пропонує рішення від провідних виробників, таких як Cisco Systems, Juniper Networks, Huawei Technologies, D-Link та MikroTik. Кожен з цих брендів має свої переваги: Cisco славиться надійністю корпоративних рішень, Juniper спеціалізується на високопродуктивному обладнанні, а компанії як D-Link та MikroTik пропонують якісні рішення за доступною ціною.

Ефективна мережева архітектура повинна забезпечувати стабільний зв'язок між усіма підрозділами організації, включаючи відділи продажів, бухгалтерії та кадрів. Критично важливо забезпечити надійний доступ до серверних ресурсів та зовнішніх мереж, при цьому дотримуючись принципів інформаційної безпеки. Правильно спроектована мережа має підтримувати як поточні потреби організації, так і можливості для майбутнього розширення. Для забезпечення роботи підсистеми у якості центрального маршрутизатора вибираємо Cisco 3745, рис.3.1.

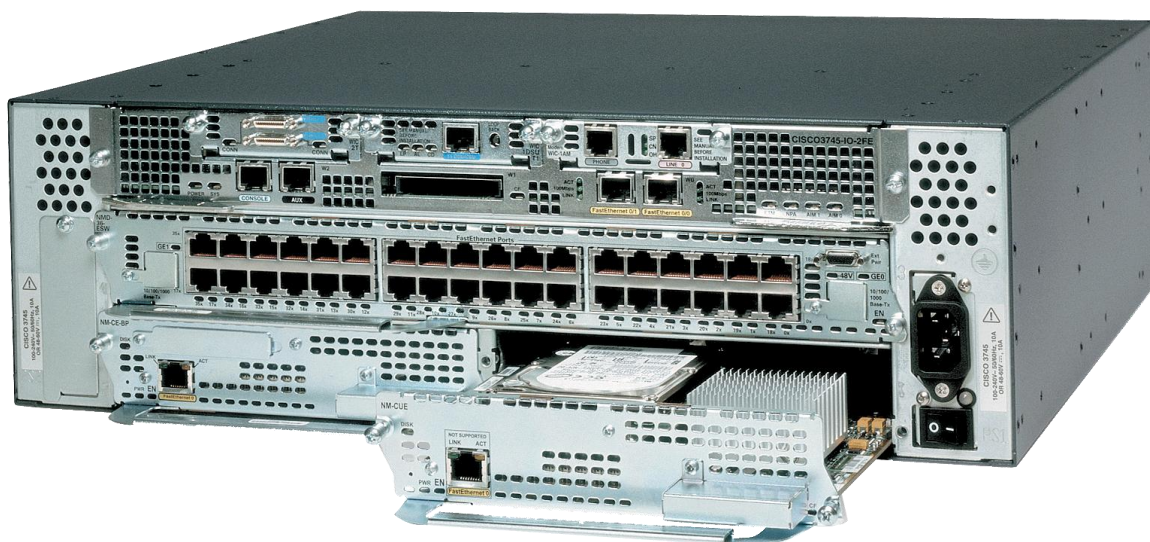


Рисунок 3.1 – Зовнішній вигляд Cisco 3745

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Для об'єднання всіх мережевих сегментів організації було обрано маршрутизатор Cisco 3745. Цей пристрій забезпечує надійну маршрутизацію між різними відділами та підтримує широкий спектр мережевих протоколів. Завдяки модульній конструкції, Cisco 3745 дозволяє гнучко налаштовувати кількість та типи мережевих інтерфейсів відповідно до потреб організації, а вбудовані функції безпеки забезпечують контроль доступу між різними сегментами мережі.

В якості комутаторів для підрозділів обираємо Brocade ICX 6450, рис.3.2.



Рисунок 3.2 – Зовнішній вигляд Brocade ICX 6450

Комутатори серії Brocade ICX 6450 широко використовуються в корпоративних мережах та спеціалізованих системах управління інфраструктурою завдяки своїй універсальності та високій продуктивності. Лінійка включає три основні моделі - ICX 6450-24, ICX 6450-48 та ICX 6450-48P, що відрізняються кількістю портів та додатковими функціональними можливостями. Ключовою особливістю цих комутаторів є гібридна портова архітектура, що поєднує стандартні мідні порти 10/100/1000 Mbps з чотирма універсальними оптичними портами SFP/SFP+. Dual-mode порти підтримують як 1 Gbps через модулі SFP, так і 10 Gbps через SFP+, забезпечуючи гнучкість в організації швидкісних uplink-з'єднань та можливості стекування для масштабування мережі. ICX 6450 знайшли своє застосування в критично важливих системах, включаючи суперкомп'ютерні кластери та розподілені обчислювальні платформи, де вони забезпечують стабільну роботу мережевої інфраструктури управління. Модель ICX 6450-48P додатково обладнана технологією Power over Ethernet, що дозволяє жити

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

підключені пристрої безпосередньо через мережевий кабель, спрощуючи розгортання IP-телефонів, точок доступу та інших мережевих компонентів.

Розроблена мережева архітектура на базі змішаного обладнання Cisco та Brocade забезпечує надійну та масштабовану інфраструктуру для ефективної роботи всіх підрозділів організації. Використання центрального маршрутизатора Cisco 3745 у поєднанні з комутаторами Brocade ICX 6450 створює стабільну основу для корпоративних комунікацій, забезпечуючи при цьому необхідний рівень безпеки та можливості для майбутнього розширення.

3.2 Розгортання мережевої інфраструктури в середовищі GNS3

Для розгортання мережі було обрано програмне середовище GNS3. GNS3 являє собою програмне рішення з відкритим вихідним кодом, призначене для емуляції мережевого обладнання різних виробників. На відміну від традиційних симуляторів, які лише імітують поведінку мережевих пристроїв, GNS3 забезпечує можливість виконання справжніх образів операційних систем у віртуальному середовищі. Це досягається завдяки інтеграції з емулятором Dynamips, розробленим Крістофом Філло у 2005 році, який став фундаментальною основою для створення GNS3 у 2007 році під керівництвом Джеремі Гроссмана.

Архітектура GNS3 базується на принципах віртуалізації та емуляції, що дозволяє відтворювати функціональність реальних мережевих пристроїв із високим ступенем аутентичності. Програма підтримує широкий спектр гіпервізорів, включаючи VirtualBox, VMware та QEMU, що забезпечує гнучкість у виборі платформи віртуалізації. Особливо важливою є можливість емуляції обладнання різних виробників, таких як Cisco, Juniper, MikroTik, Arista та Vyatta, що робить GNS3 універсальним інструментом для моделювання гетерогенних мережевих середовищ. Технічна досконалість GNS3 проявляється у його здатності забезпечувати аутентичний досвід роботи з командним рядком мережевого обладнання. Користувачі мають можливість виконувати ті самі команди та конфігурації, що й на реальних пристроях, що є критично важливим для формування професійних компетенцій. Інтеграція з Wireshark дозволяє проводити

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

детальний аналіз мережевого трафіку, що суттєво розширює можливості дослідження протоколів та діагностики мережевих проблем.

Професійне застосування GNS3 охоплює широкий спектр задач, від проектування нових мережевих рішень до підготовки до сертифікаційних іспитів. Мережеві інженери використовують програму для моделювання та тестування архітектури перед впровадженням у продуктивному середовищі, що дозволяє виявити потенційні проблеми та оптимізувати конфігурації на етапі планування. Підтримка Python API відкриває можливості для автоматизації процесів конфігурації та управління, що відповідає сучасним тенденціям у галузі мережевих технологій.

В результаті проведених досліджень було створено мережну інфраструктуру за розробленою діаграмою, яка представлена на рис.3.3.

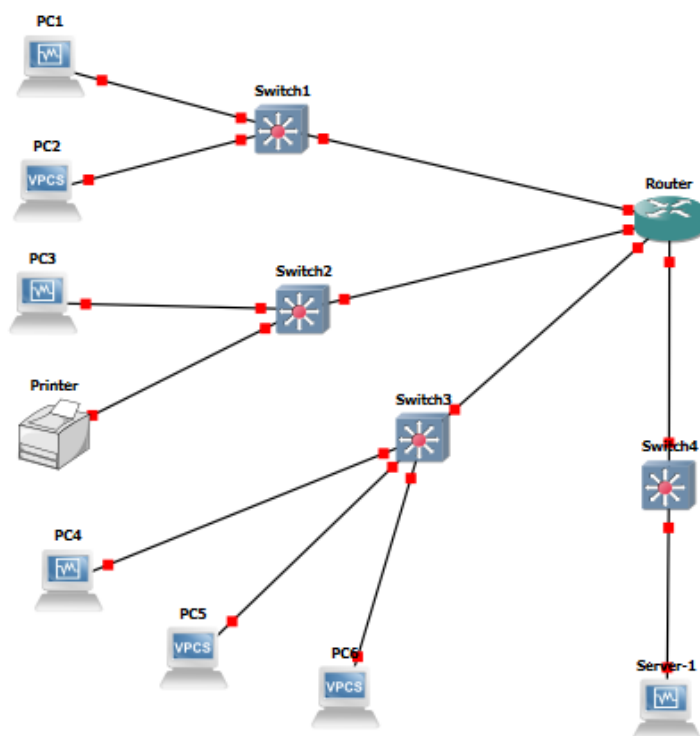


Рисунок 3.3 – Удосконалена мережа, створена в GNS3

Мережа включає в себе центральний маршрутизатор Cisco 3745, 4 комутатори Brocade ICX 6450, 6 користувацьких комп'ютерів, принтер та сервер.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Для економії ресурсів, в кожній групі додано лише одну віртуальну машину Windows, інші користувацькі комп'ютери представлено за допомогою VPCS (Virtual PC Simulator) – спеціалізованого програмного засобу для емуляції ресурсоекономних персональних комп'ютерів у мережевому середовищі. Програма підтримує протоколи DHCP та ICMP для діагностики мережі, споживаючи лише 2 мегабайти оперативної пам'яті на екземпляр та функціонуючи без потреби у додаткових образах операційних систем.

Таблиця 3.1.

Описова таблиця мережі

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Router	f0/0	Switch1	e0/0
	f0/1	Switch2	e0/0
	f1/0	Switch3	e0/0
	f1/1	Switch4	e0/0
Switch1	e0/0	Router	f0/0
	e0/1	PC1	e0
	e0/2	PC2	e0
Switch2	e0/0	Router	f0/1
	e0/1	PC3	e0
	e0/2	Printer	e0
Switch3	e0/0	Router	e0/0
	e0/1	PC4	e0

	e0/2	PC5	e0
	e0/3	PC6	e0
Switch4	e0/0	Router	f1/1
	e0/1	Server1	e0
PC1	e0	Switch1	e0/1
PC2	e0	Switch1	e0/2
PC3	e0	Switch2	e0/1
PC4	e0	Switch3	e0/1
PC5	e0	Switch3	e0/2
PC6	e0	Switch3	e0/3
Printer	e0	Switch2	e0/2
Server	e0	Switch4	e0/1

Сервер працює на ОС Windows Server 2019 – спеціалізованій версії Windows, адаптованій для корпоративних потреб підприємств. Windows Server підтримує значно ширший спектр обладнання порівняно з домашніми ОС, що зумовлено необхідністю обслуговування розгалужених мережевих інфраструктур та функціонування численних віртуальних машин.

3.3 Конфігурація мережевого обладнання та налаштування моніторингу

Роботу з налаштування мережі розпочинаємо з розроблення таблиці адресації (таблиця 3.2), яка містить необхідну інформацію про IP-адреси, маски підмереж, шлюзи за замовчуванням та інтерфейси пристроїв. Ця таблиця є основою для подальшої конфігурації IP-адресації на всіх мережевих пристроях – маршрутизаторах, комутаторах та кінцевих пристроях. Відповідно до даних, зазначених у таблиці, здійснюється налаштування кожного інтерфейсу з метою

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

забезпечення коректного функціонування мережі, зокрема взаємодії між підмережами, маршрутизації та доступу до зовнішніх ресурсів.

Таблиця 3.2.

Таблиця адресації.

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
Мережа А	-	192.168.1.0	255.255.255.0	/24
Мережа В	-	192.168.2.0	255.255.255.0	/24
Мережа С	-	192.168.3.0	255.255.255.0	/24
Мережа D	-	192.168.4.0	255.255.255.0	/24
Router	f0/0	192.168.1.1	255.255.255.0	/24
	f0/1	192.168.2.1	255.255.255.0	/24
	f1/0	192.168.3.1	255.255.255.0	/24
	f1/1	192.168.4.1	255.255.255.0	/24
Switch1	vlan1	192.168.1.11	255.255.255.0	/24
	Шлюз за замовч.	192.168.1.1	255.255.255.0	/24
Switch2	vlan1	192.168.2.11	255.255.255.0	/24
	Шлюз за замовч.	192.168.2.1	255.255.255.0	/24
Switch3	vlan1	192.168.3.11	255.255.255.0	/24
	Шлюз за замовч.	192.168.3.1	255.255.255.0	/24
Switch4	vlan1	192.168.4.11	255.255.255.0	/24
	Шлюз за замовч.	192.168.4.1	255.255.255.0	/24
PC1	vlan1	192.168.1.21	255.255.255.0	/24
	Шлюз за замовч.	192.168.1.1	255.255.255.0	/24
PC2	vlan1	192.168.1.22	255.255.255.0	/24
	Шлюз за замовч.	192.168.1.1	255.255.255.0	/24
PC3	vlan1	192.168.2.21	255.255.255.0	/24
	Шлюз за замовч.	192.168.2.1	255.255.255.0	/24
PC4	vlan1	192.168.3.21	255.255.255.0	/24

Пристрій	Інтерфейс	ІР-адреса	Маска	Префікс
	Шлюз за замовч.	192.168.3.1	255.255.255.0	/24
PC5	vlan1	192.168.3.22	255.255.255.0	/24
	Шлюз за замовч.	192.168.3.1	255.255.255.0	/24
PC6	vlan1	192.168.3.23	255.255.255.0	/24
	Шлюз за замовч.	192.168.3.1	255.255.255.0	/24
Printer	vlan1	192.168.2.22	255.255.255.0	/24
	Шлюз за замовч.	192.168.2.1	255.255.255.0	/24
Server	vlan1	192.168.4.21	255.255.255.0	/24
	Шлюз за замовч.	192.168.4.1	255.255.255.	/24

Для маршрутизатора необхідно призначити ІР-адреси всім активним інтерфейсам відповідно до розробленої схеми адресації.

```

Router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#int f0/0
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#ex
Router1(config)#in
*Mar 1 00:08:39.415: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:08:40.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router1(config)#int f0/1
Router1(config-if)#ip address 192.168.2.1 255.255.255.0
Router1(config-if)#no shut
Router1(config-if)#
*Mar 1 00:09:08.127: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar 1 00:09:09.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router1(config-if)#ex

```

Рисунок 3.4 - Налаштування адрес портів маршрутизатора.

Для того, щоб присвоїти ІР-адреси інтерфейсам другого рівня, потрібно відключити функцію switchport.

```

Router1(config)#int f1/0
Router1(config-if)#ip address 192.168.3.1
% Incomplete command.

Router1(config-if)#ip address 192.168.3.1 255.255.255.0

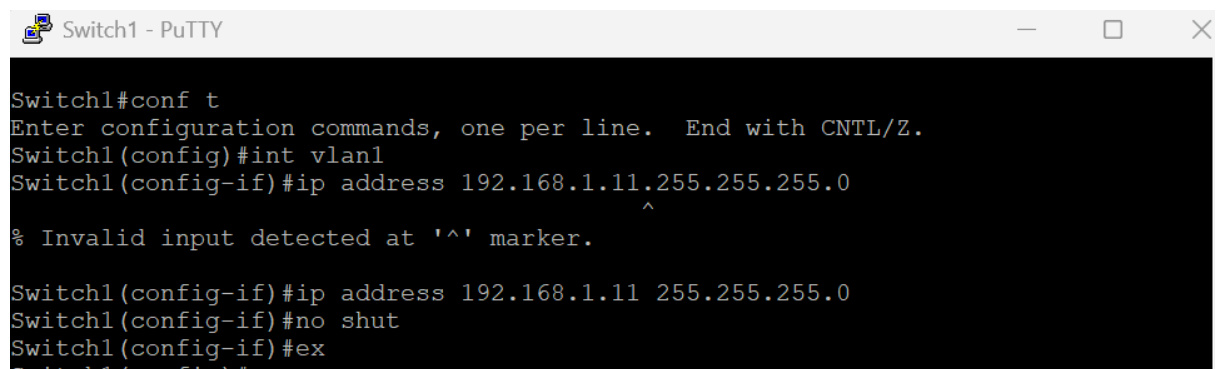
% IP addresses may not be configured on L2 links.

Router1(config-if)#no switchport
Router1(config-if)#ip address 192.168.3.1 255.255.255.0
Router1(config-if)#no
*Mar 1 00:11:08.819: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Router1(config-if)#no shut
Router1(config-if)#

```

Рисунок 3.5 – Налаштування адреси для інтерфейсу другого рівня

На комутаторах призначаються IP-адреси та маски підмережі для кожного комутатора згідно з таблицею адресації.



```

Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#int vlan1
Switch1(config-if)#ip address 192.168.1.11.255.255.255.0
% Invalid input detected at '^' marker.

Switch1(config-if)#ip address 192.168.1.11 255.255.255.0
Switch1(config-if)#no shut
Switch1(config-if)#ex
Switch1(config-if)#

```

Рисунок 3.5 – Налаштування адресації на Switch1, на інших комутаторах було проведено аналогічні дії.

На кінцевих пристроях (робочі станції, сервер, принтер) також налаштовується IP-конфігурація з указанням відповідних шлюзів за замовчуванням для забезпечення міжмережевої комунікації.

```

PC2> ip 192.168.1.22 255.255.255.0 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.22 255.255.255.0 gateway 192.168.1.1

```

Рисунок 3.6 – Налаштування адресації на VPCS.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

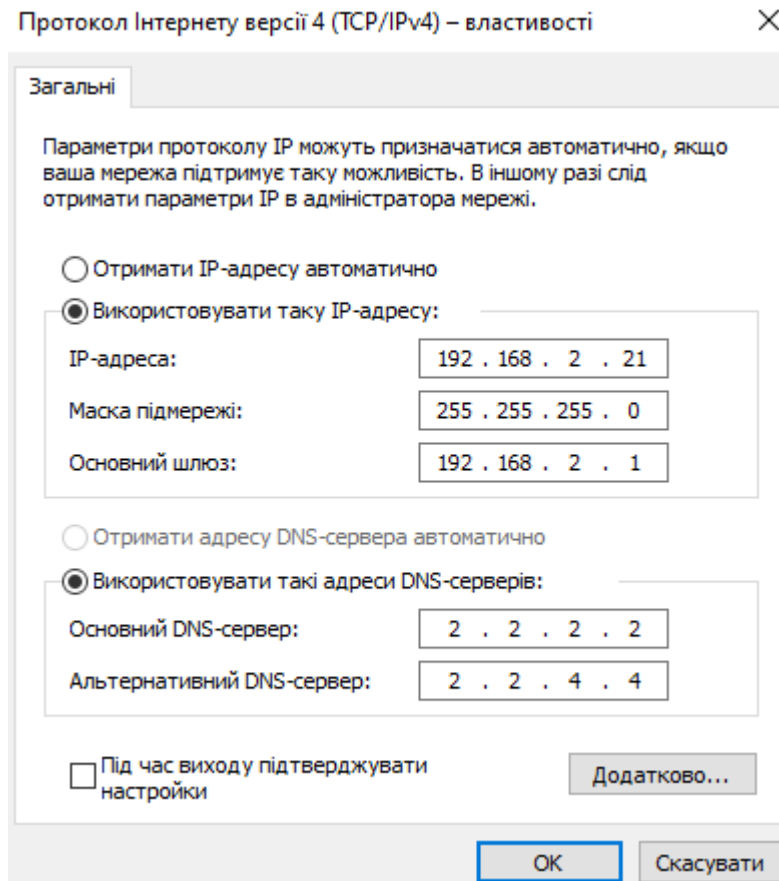


Рисунок 3.7. Налаштування адресації на віртуальній машині

Після завершення базової конфігурації проводиться комплексна перевірка зв'язку між усіма елементами мережі. Тестування включає:

- Перевірку зв'язку між маршрутизатором та комутаторами

```
Switch1#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 9/22/60 ms
Switch1#
```

Рисунок 3.8 – Зв'язок між маршрутизатором та комутаторами працює.

- Тестування з'єднання між комутаторами в різних підмережах

```
Switch4#ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 13/19/23 ms
Switch4#write memory
```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Рисунок 3.9 – Зв’язок між комутаторами в різних підмережах працює.

- Перевірку доступності кінцевих пристроїв з маршрутизатора

```
Router1#ping 192.168.2.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/16/44 ms
Router1#
```

Рисунок 3.10 – Перевірка зв’язку між маршрутизатором та робочими станціями.

- Тестування міжмережевої комунікації між робочими станціями в різних підмережах

```
C:\Users\Student>ping 192.168.3.21

Pinging 192.168.3.21 with 32 bytes of data:
Reply from 192.168.3.21: bytes=32 time<1ms TTL=128
Reply from 192.168.3.21: bytes=32 time<1ms TTL=128
Reply from 192.168.3.21: bytes=32 time<1ms TTL=128
Reply from 192.168.3.21: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 3.11 – Перевірка зв’язку між робочими станціями в різних підмережах

Успішне проходження всіх тестів підтверджує коректність налаштування мережевої інфраструктури та готовність до впровадження додаткових сервісів.

Для здійснення моніторингу LLMNR трафіку в мережі було обрано технологію RSPAN (Remote Switch Port Analyzer). RSPAN є розвитком традиційної технології SPAN, що дозволяє здійснювати моніторинг мережевого трафіку між різними комутаторами в мережі. На відміну від локального SPAN, де джерело та пункт призначення знаходяться на одному комутаторі, RSPAN забезпечує можливість централізованого збору та аналізу трафіку з розподілених джерел [5].

Основою функціонування RSPAN є концепція спеціалізованої VLAN, що виконує роль транспортного каналу для передачі дубльованого трафіку між

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

комутаторами. Ця RSPAN VLAN має унікальні характеристики, які відрізняють її від звичайних VLAN у корпоративній мережі. Зокрема, комутатори не здійснюють навчання MAC-адрес на портах, що належать до RSPAN VLAN, що запобігає порушенню нормального процесу комутації. Весь трафік у цій VLAN передається методом флудингу на всі порти, забезпечуючи доставку моніторингових даних до пункту призначення.

Процес конфігурації RSPAN включає кілька етапів, що вимагають координованих дій на всіх залучених комутаторах: створення RSPAN VLAN - необхідно створити та позначити RSPAN VLAN на всіх комутаторах мережі, використовуючи спеціальну команду `remote-span`; конфігурація trunk-портів - налаштування trunk-портів між комутаторами для передачі RSPAN VLAN, що створює фізичний шлях для транспортування моніторингового трафіку; налаштування `source session` - на джерельному комутаторі створюється RSPAN `source session`, де визначаються порти або інтерфейси, трафік яких підлягає моніторингу; конфігурація `destination session` - цільовий комутатор конфігурується з RSPAN `destination session`, де RSPAN VLAN виступає джерелом, а конкретний фізичний порт – пунктом призначення [3, 6].

```
Switch1(config)#vlan 100
Switch1(config-vlan)#remote-span
Switch1(config-vlan)#name LLNMR
Switch1(config-vlan)#exit
Switch1(config)#int e0/0
Switch1(config-if)#switchport trunk allowed vlan add 100
Switch1(config-if)#ex
Switch1(config)#monitor session 1 source interface ethernet 0/1
Switch1(config)#monitor session 1 source interface ethernet 0/2
Switch1(config)#monitor session 1 destination remote vlan 100
Switch1(config)#exit
```

Рисунок 3.12 – Налаштування RSPAN на комутаторах.

RSPAN надає значні переваги для організації мережевого моніторингу в розподілених корпоративних мережах. Централізація систем захоплення трафіку дозволяє зменшити кількість необхідного спеціалізованого обладнання та спростити процедури аналізу мережевої активності.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Водночас технологія має певні обмеження: підвищене навантаження на міжкомутаторні з'єднання може негативно вплинути на загальну продуктивність мережі, особливо при моніторингу високошвидкісних інтерфейсів або великої кількості портів одночасно [4].

RSPAN представляє ефективний інструмент для організації розподіленого моніторингу мережевого трафіку, що особливо актуально для великих корпоративних мереж з розгалуженою топологією. Правильна реалізація цієї технології дозволяє досягти оптимального балансу між потребами моніторингу та збереженням продуктивності мережевої інфраструктури [20].

Висновки до третього розділу

У рамках даного розділу було успішно спроектовано та реалізовано корпоративну мережеву інфраструктуру для організації з декількома відділами, використовуючи сучасне обладнання провідних виробників. Розроблена архітектура продемонструвала ефективність поєднання надійних рішень від Cisco Systems і Brocade Networks.

Центральним елементом мережі обрано маршрутизатор Cisco 3745, який забезпечує стабільну міжмережеву маршрутизацію завдяки своїй модульній конструкції та вбудованим функціям безпеки. Використання комутаторів серії Brocade ICX 6450 виявилось оптимальним рішенням для організації підрозділів, оскільки ці пристрої поєднують високу продуктивність з гнучкою гібридною портовою архітектурою, що включає як стандартні мідні порти, так і універсальні оптичні SFP/SFP+ інтерфейси.

Практична реалізація мережі в емуляційному середовищі GNS3 підтвердила правильність обраного підходу. GNS3 довів свою ефективність як інструмент для моделювання складних мережевих топологій, забезпечуючи аутентичний досвід роботи з командним рядком реального обладнання. Інтеграція з різними гіпервізорами та підтримка широкого спектру виробників мережевого обладнання

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

робить цю платформу універсальним рішенням для проектування та тестування корпоративних мереж.

Створена мережева топологія включає чотири окремі підмережі (192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24), що забезпечує логічне розділення трафіку різних відділів організації. Кожна підмережа обслуговує конкретні функціональні потреби: мережа А призначена для відділу продажів, мережа В - для бухгалтерії з інтегрованим принтером, мережа С обслуговує відділ кадрів, а мережа D забезпечує роботу серверної інфраструктури.

Комплексне тестування зв'язку підтвердило коректність налаштування всіх компонентів мережі. Успішна перевірка міжмережевої комунікації між різними підрозділами демонструє правильність конфігурації маршрутизації та IP-адресації. Використання технології VPCS для емуляції користувацьких робочих станцій дозволило значно оптимізувати споживання системних ресурсів без втрати функціональності тестування.

Особливу увагу приділено впровадженню системи моніторингу на базі технології RSPAN (Remote Switch Port Analyzer). Ця технологія забезпечує централізований збір і аналіз мережевого трафіку з розподілених джерел, що є критично важливим для забезпечення інформаційної безпеки та діагностики мережевих проблем. Конфігурація RSPAN вимагала координованих дій на всіх комутаторах мережі, включаючи створення спеціалізованої RSPAN VLAN, налаштування trunk-портів та конфігурацію source і destination сесій.

Реалізована мережева архітектура забезпечує надійну основу для корпоративних комунікацій з дотриманням принципів масштабованості та безпеки. Модульна структура дозволяє легко розширювати мережу при зростанні потреб організації, а впроваджені системи моніторингу забезпечують необхідний рівень контролю над мережевою активністю.

Отримані результати підтверджують ефективність обраного підходу до проектування корпоративних мереж та демонструють практичну цінність використання емуляційних середовищ для тестування і верифікації мережевих рішень перед їх впровадженням у продуктивному середовищі.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

ВИСНОВКИ

У рамках виконання дипломної роботи було проведено комплексний аналіз протоколу LLMNR у контексті корпоративної мережевої безпеки та розроблено практичні рекомендації щодо мінімізації пов'язаних ризиків.

1. Дослідження протоколу LLMNR виявило його подвійну природу: з одного боку, він забезпечує корисну функціональність локального розв'язання імен у Windows-середовищах, особливо в сценаріях втрати зв'язку з DNS-серверами, з іншого - створює значні вразливості безпеки через можливість перехоплення та підміни multicast-запитів. Аналіз показав, що LLMNR-атаки можуть призвести до компрометації облікових даних, латерального переміщення в мережі та повної компрометації домену Active Directory.

2. Розроблена система захисних заходів базується на принципах мережевої сегментації, активного моніторингу та контролю доступу. Запропонована архітектура корпоративної мережі з фізичним розділенням відділів суттєво обмежує поширення LLMNR-трафіку та локалізує потенційні загрози в межах окремих сегментів.

3. Практична реалізація захисних заходів у емуляційному середовищі GNS3 підтвердила ефективність обраного підходу. Впровадження технології RSPAN забезпечило централізований моніторинг мережевого трафіку, що є критично важливим для своєчасного виявлення LLMNR-атак. Комбінація контролю MAC-адрес, NetFlow моніторингу та систем захоплення пакетів створює багаторівневу систему захисту.

4. Отримані результати підтверджують, що ефективний захист від LLMNR-атак вимагає системного підходу, який поєднує технічні заходи (сегментація мережі, моніторинг трафіку), організаційні процедури (контроль доступу, аудит) та стратегічне планування з урахуванням еволюції технологій розв'язання імен. Особливо важливим є розуміння того, що з часом Microsoft відмовляється від LLMNR на користь mDNS, що вимагає довгострокового планування міграційних стратегій.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

5. Дослідження демонструє практичну цінність використання емуляційних середовищ для тестування мережесих рішень безпеки та підтверджує необхідність проактивного підходу до захисту корпоративних мереж від сучасних векторів атак.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Andress J. Building a Practical Information Security Program / J. Andress, M. Leary. 2017, 279 p.
2. Büyüközkan G. Cybersecurity maturity model: Systematic literature review and a proposed model / G. Büyüközkan, M. Güler // Technological Forecasting and Social Change, 347 p.
3. Capturing Traffic on Cisco Routers (Електронний ресурс). URL: <https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKF9EAO/capturing-traffic-on-cisco-routers-rite-and-epc-features> (дата звернення: 17.06.2025).
4. Configure traffic mirroring with a Remote SPAN (RSPAN) port (Електронний ресурс). URL: <https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/traffic-mirroring/configure-mirror-rspan> (дата звернення: 20.06.2025).
5. Configuring SNMP Support (Електронний ресурс). URL: <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12.html> (дата звернення: 11.06.2025).
6. Configuring SPAN and RSPAN (Електронний ресурс). URL: https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_01101101.html#ID62 (дата звернення: 08.06.2025).
7. Faircloth J. Enterprise Applications Administration / J. Faircloth. 2014 284 p.
8. Hunt R. Encyclopedia of Information Systems / R. Hunt, J. Vargo. 2003, 476p.
9. Knapp E. D. Industrial Network Security (Second Edition) / E. D. Knapp, J. T. Langill. 2015 368 p.
10. Link Local Multicast Name Resolution Protocol (Електронний ресурс). URL: <https://winprotocoldocs-bhdugrduyduf5h2e4.b02.azurefd.net/MS-LLMNRP/%5bMS-LLMNRP%5d.pdf> (дата звернення: 13.06.2025).
11. Link-Local Multicast Name Resolution (LLMNR) : RFC 4795 (Електронний ресурс). URL: <https://www.rfc-editor.org/rfc/rfc4795.html> (дата звернення: 15.06.2025).

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

12. LLMNR & NBT-NS: What it is and how to disable it (Електронний ресурс). URL: <https://blogs.dsu.edu/digforce/2023/08/04/llmnr-nbt-ns-what-it-is-and-how-to-disable-it/> (дата звернення: 02.06.2025).
13. LLMNR Poisoning : MITRE ATT&CK (Електронний ресурс). URL: <https://attack.mitre.org/techniques/T1557/001/> (дата звернення: 24.06.2025).
14. Network Intrusion Analysis and Countermeasures (Електронний ресурс). URL: [https://www.sciencedirect.com/science/article/abs/pii/B9780128054727000061?](https://www.sciencedirect.com/science/article/abs/pii/B9780128054727000061?via%3Dihub)
[via%3Dihub](https://www.sciencedirect.com/science/article/abs/pii/B9780128054727000061?via%3Dihub) (дата звернення: 09.06.2025).
15. Network Segmentation : MITRE ATT&CK (Електронний ресурс). URL: <https://attack.mitre.org/mitigations/M1031/> (дата звернення: 05.06.2025).
16. Password policy recommendations for Microsoft 365 (Електронний ресурс). URL: <https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide> (дата звернення: 03.06.2025).
17. Shinder L. Scene of the Cybercrime (Second Edition) / L. Shinder, M. Cross. 2008, 315p.
18. Shinder T. W. Dr. Tom Shinder's Configuring ISA Server 2004 / T. W. Shinder, D. L. Shinder. 2005, 325 p.
19. Sun F. Unsupervised field segmentation of unknown protocol messages / F. Sun, S. Wang, C. Zhang, H. Zhang // Computer Communications. 2019. Vol. 146. P. 121-130.
20. Understanding SPAN, RSPAN, and ERSPAN (Електронний ресурс). URL: <https://community.cisco.com/t5/networking-knowledge-base/understanding-span-rspan-and-erspan/ta-p/3144951> (дата звернення: 07.06.2025).
21. What is incident response? (Електронний ресурс). URL: <https://www.ibm.com/think/topics/incident-response> (дата звернення: 22.06.2025).
22. What is network design? (Електронний ресурс). URL: <https://www.cisco.com/site/us/en/learn/topics/networking/what-is-network-design.html> (дата звернення: 19.06.2025).
23. Yang W. Heterogeneous cross-side network effects on peer-to-peer platforms: Implications of nonprofessional suppliers and professional suppliers / W. Yang, P. Song, Y. Ruan, 415 p.

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

ДОДАТКИ

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

Описова таблиця мережі

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Router	f0/0	Switch1	e0/0
	f0/1	Switch2	e0/0
	f1/0	Switch3	e0/0
	f1/1	Switch4	e0/0
Switch1	e0/0	Router	f0/0
	e0/1	PC1	e0
	e0/2	PC2	e0
Switch2	e0/0	Router	f0/1
	e0/1	PC3	e0
	e0/2	Printer	e0
Switch3	e0/0	Router	e0/0
	e0/1	PC4	e0
	e0/2	PC5	e0
	e0/3	PC6	e0
Switch4	e0/0	Router	f1/1
	e0/1	Server1	e0
PC1	e0	Switch1	e0/1

PC2	e0	Switch1	e0/2
PC3	e0	Switch2	e0/1
PC4	e0	Switch3	e0/1
PC5	e0	Switch3	e0/2
PC6	e0	Switch3	e0/3
Printer	e0	Switch2	e0/2
Server	e0	Switch4	e0/1

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Конфігураційний файл Router1

```

Router1#show run
Building configuration...

Current configuration : 1635 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
no ip domain lookup
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0
no ip address
shutdown
clock rate 2000000
!

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
no switchport
ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet1/1
no switchport
ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet1/2
!
interface FastEthernet1/3
!
interface FastEthernet1/4
!
interface FastEthernet1/5
!
interface FastEthernet1/6
!
interface FastEthernet1/7
!
interface FastEthernet1/8
!
interface FastEthernet1/9
!
interface FastEthernet1/10
!
interface FastEthernet1/11
!
interface FastEthernet1/12
!
interface FastEthernet1/13
!
interface FastEthernet1/14
!
interface FastEthernet1/15
!
interface Vlan1
no ip address
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```

!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login
!
!
end
Конфігураційний файл Switch1
Switch1#show run
Building configuration...

Current configuration : 1712 bytes
!
! Last configuration change at 04:07:40 UTC Mon Jun 30 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
no ip domain-lookup

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex half
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.2.0 255.255.255.0 192.168.1.1
ip route 192.168.3.0 255.255.255.0 192.168.1.1
ip route 192.168.4.0 255.255.255.0 192.168.1.1
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
monitor session 1 source interface Et0/1 - 2
monitor session 1 destination remote vlan 100
!
end

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

Конфігураційний файл Switch2

Switch2#show run

Building configuration...

Current configuration : 1708 bytes

!

! Last configuration change at 04:07:41 UTC Mon Jun 30 2025

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname Switch2

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

!

!

no ip icmp rate-limit unreachable

!

!

no ip domain-lookup

ip cef

no ipv6 cef

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

!

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

duplex half

!

interface Ethernet0/1

!

interface Ethernet0/2

!

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.2.11 255.255.255.0
!
 ip default-gateway 192.168.2.1
 ip forward-protocol nd
!
!
 no ip http server
 no ip http secure-server
 ip route 192.168.1.0 255.255.255.0 192.168.2.1
 ip route 192.168.3.0 255.255.255.0 192.168.2.1
 ip route 192.168.4.0 255.255.255.0 192.168.2.1
!
!
 control-plane
!
!
 line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

login
!
!
monitor session 1 source interface Et0/1
monitor session 1 destination remote vlan 100
!
end

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

Конфігураційний файл Switch3

Switch3#show run

Building configuration...

Current configuration : 1712 bytes

!

! Last configuration change at 04:07:43 UTC Mon Jun 30 2025

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname Switch3

!

boot-start-marker

boot-end-marker

!

!

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

!

!

no ip icmp rate-limit unreachable

!

!

no ip domain-lookup

ip cef

no ipv6 cef

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

ip tcp synwait-time 5

!

!

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

duplex full

!

interface Ethernet0/1

!

interface Ethernet0/2

!

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.3.11 255.255.255.0
!
 ip default-gateway 192.168.3.1
 ip forward-protocol nd
!
!
 no ip http server
 no ip http secure-server
 ip route 192.168.1.0 255.255.255.0 192.168.3.1
 ip route 192.168.2.0 255.255.255.0 192.168.3.1
 ip route 192.168.4.0 255.255.255.0 192.168.3.1
!
!
 control-plane
!
!
 line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

login
!
!
monitor session 1 source interface Et0/1 - 3
monitor session 1 destination remote vlan 100
!
end

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Конфігураційний файл Switch4

Switch4#show run
Building configuration...

```
Current configuration : 1708 bytes
!
! Last configuration change at 04:07:45 UTC Mon Jun 30 2025
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
!
no ip icmp rate-limit unreachable
!
!
no ip domain-lookup
ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex full
!
interface Ethernet0/1
!
interface Ethernet0/2
!
```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		71

```

interface Ethernet0/3
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 192.168.4.11 255.255.255.0
!
 ip default-gateway 192.168.4.1
 ip forward-protocol nd
!
!
 no ip http server
 no ip http secure-server
 ip route 192.168.1.0 255.255.255.0 192.168.4.1
 ip route 192.168.2.0 255.255.255.0 192.168.4.1
 ip route 192.168.3.0 255.255.255.0 192.168.4.1
!
!
 control-plane
!
!
 line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
 line vty 0 4

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

login
!
!
monitor session 1 destination interface Et3/3
monitor session 1 source remote vlan 100
!
end

```

		Бордюг О.О.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		