

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 від інсайдерських атак Windows-мережі
на базі Active Directory»

Виконав студентка 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Вероніка Єсипенко

Керівник доцент кафедр КІ та КБ, к.пед.н

 Олена Головня

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

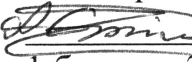
 Андрій Єфіменко

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Єсипенко Вероніка Ігорівна

Тема роботи: «Проект підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory»

затверджена Наказом університету від 1 березня 2023 р. №99/с

Термін здачі студентом закінченої роботи 10 червня 2023 р.

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

- мережа організації;
- методи захисту від інсайдерських атак ;
- застосування засобів Active Directory для реалізації захисту Windows-мережі від інсайдерських атак.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7200 Series VXR
2. Cisco Catalyst 2960-24LC-S
3. Active Directory
4. Windows 10

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			

2			
3	Головня О. С.	29.03.2023 	29.03.2023 

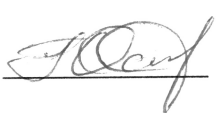
Студент  Єсипенко В. І.

Керівник  Головня О. С.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	01.03.2023	Виконано
2	Аналіз літературних джерел	03.03.2023 – 15.03.2023	Виконано
3	Аналіз об'єкта дослідження	16.03.2023	Виконано
4	Постановка задачі дослідження	19.03.2023	Виконано
5	Розробка структурної моделі	25.03.2023 – 04.04.2023	Виконано
6	Розрахунок параметрів адресації	05.04.2023	Виконано
7	Вибір технології для реалізації	13.04.2023	Виконано
8	Розробка захищеної КМ	23.05.2023	Виконано
9	Налаштування мережі	27.05.2023	Виконано
10	Налагодження Active Directory	03.05.2023	Виконано
11	Оформлення пояснювальної записки	11.06.2023	Виконано
12	Оформлення презентації	22.06.2023	Виконано
13	Захист	28.06.2023	Виконано

Студент  Єсипенко В. І.

Керівник  Головня О. С.

АНОТАЦІЯ

Кваліфікаційна робота складається з проєкту підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory, його реалізацію та пояснювальної записки до нього.

Пояснювальна записка містить 53 сторінки та 48 ілюстрацій. Список використаних джерел містить 11 найменувань та розміщений на 1 сторінці.

Метою роботи є розробка проєкту підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory.

В роботі було описане мережеве обладнання, створено проєкт підсистеми та налаштовано його. Налаштовані методи захисту за допомогою групових політик Active Directory та наведено результати тестування.

Ключові слова: WINDOWS, ACTIVE DIRECTORY, ІНСАЙДЕР, ІНСАЙДЕРСЬКІ АТАКИ, ЗАХИСТ.

KKIK.KP.B – 125 – 5 – ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.	Єсипенко В. І.	10.06.23			Проєкт підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory	Літ.	Арк.
Керівник	Головня О.С.	10.06.23					Аркуші
Реценз.	Єфіменко А.А.	10.06.23				4	53
Затверд.	Єфіменко А.А.	10.06.23				ФІКТ, Гр. КБ-19-1	

ANNOTATION

The qualification work consists of the project of the subsystem of protection against insider attacks of the Windows network based on Active Directory, its implementation and an explanatory note to it.

The explanatory note contains 53 pages and 48 illustrations. The list of used sources contains 11 names and is placed on 1 page.

The purpose of the work is to develop a project of the protection subsystem against insider attacks of the Windows network based on Active Directory.

The work described network equipment, created a subsystem project and configured it. Configured protection methods using Active Directory Group Policies and test results.

Keywords: WINDOWS, ACTIVE DIRECTORY, INSIDER, INSIDER ATTACKS, PROTECTION.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ВІДОМОСТІ ПРО ІНСАЙДЕРСЬКІ АТАКИ ТА МЕТОДИ ЗАХИСТУ	9
1.1 Інсайдерські атаки та їх види.....	9
1.2 Методи виявлення інсайдерських атак та інструменти для захисту	11
1.3 Вразливості мережі на базі Windows.....	13
РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК WINDOWS-МЕРЕЖІ	14
2.1 Вибір обладнання для організації роботи мережі	14
2.2 Розробка моделі загроз для компанії	16
2.3 Розробка політики безпеки для співробітників.....	19
2.4 Розробка проєкту мережі.....	20
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ WINDOWS-МЕРЕЖІ	25
3.1 Налаштування обладнання мережі.....	25
3.2 Налаштування Active Directory на базі Windows Server 2019.....	28
3.3 Тестування та оцінка ефективності підсистеми.....	39
ВИСНОВКИ.....	42
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	43
ДОДАТКИ.....	44
Додаток А Схема побудованої мережі	45
Додаток Б Лістинг конфігурації пристроїв	46

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

AD – Active Directory

SSH – Secure Shell

OSPF – Open Shortest Path First

EIGRP – Enhanced Interior Gateway Routing Protocol

DoS – Disk Operating System

VLAN – Virtual Local Area Network

IP – Internet Protocol

SAM – Security Accounts Manager

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Важко уявити у ХХІ сторіччі компанії та й звичайних людей без інформаційних систем. Це є нашою щоденною потребою: для роботи, навчання, отримання інформації та для відпочинку. Та з розвитком технологій, ризик інсайдерських атак на підприємства зростає, тому на сьогоднішній день компанії все більше стають зацікавлені у захисті своєї мережі, щоб не допустити виток важливої та конфіденційної інформації.

Актуальність теми. Отже, захист даних є важливою складовою, тому що організації, які обслуговують людей, зберігають усю інформацію на пристроях(сервери, комп'ютери і т.д.). Тому постає питання про збереження цих конфіденційних даних, щоб не відбулося несанкціонованого доступу як зі сторони злоумисників, так і зі сторони самих співробітників.

Метою кваліфікаційної роботи є розробка проєкту підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory.

Встановлена мета обумовлює наступні завдання:

- обґрунтувати необхідність розробки системи захисту від інсайдерських атак Windows-мережі на базі Active Directory;
- розробити проєкт підсистеми захисту від інсайдерських атак;
- налагодити та протестувати систему захисту від інсайдерських атак

Об'єктом дослідження є методи захисту від інсайдерських атак.

Предметом дослідження є застосування засобів Active Directory для реалізації захисту Windows-мережі від інсайдерських атак.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ВІДОМОСТІ ПРО ІНСАЙДЕРСЬКІ АТАКИ ТА МЕТОДИ ЗАХИСТУ

1.1 Інсайдерські атаки та їх види

Інсайдер – працівник компанії, який користуючись доступом до конфіденційної інформації, розміщеної у комп'ютерній мережі установи, використовує її для нанесення збитків компанії або отримання грошової нагороди.

Такі порушники поділяються на такі категорії:

- лояльні інсайдери (недбалі та маніпульовані);
- скривджені та нелояльні інсайдери;
- мотивовані ззовні (мотивовані фінансово та впроваджені);
- інші порушники (ті, що мають на меті вплинути на вартість акцій підприємства).

Нам відомо, що інформація може бути відкрита та конфіденційна. Та саме конфіденційна інформація є ціллю зловмисників. У табл. 1.1 наведено основні категорії зловмисних атак. Нижче буде наведена таблиця з типовими видами атак[2].

Таблиця 1.1 – Види атак

Категорія атаки	Опис
атака підслуховування	Атака підслуховування полягає у тому, що загрозовий суб'єкт перехоплює та прослуховує мережевий трафік. Ця атака також називається сніфінгом, або шпигунством.
атака модифікації даних	Атаки на модифікацію даних відбуваються, коли зловмисник захопив трафік підприємства та змінив дані в пакетах без відома відправника чи одержувача.
атака підробки IP-адреси	Атака зі спуфінгом IP-адреси полягає в тому, що зловмисник створює IP-пакет, який, здається, походить із дійсної адреси всередині корпоративної внутрішньої мережі.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

Категорія атаки	Опис
атаки на основі паролів	Атаки на основі пароля відбуваються, коли загроза отримує облікові дані для дійсного облікового запису користувача. Зловмисники потім використовують цей обліковий запис для отримання списків інших користувачів і інформації про мережу. Вони також можуть змінювати конфігурації сервера та мережі, а також змінювати, перенаправляти або видаляти дані.
атака на відмову в обслуговуванні (DoS).	DoS-атака перешкоджає нормальному використанню комп'ютера або мережі дійсними користувачами. Після отримання доступу до мережі DoS-атака може призвести до збою програм або мережевих служб. DoS-атака також може заповнити комп'ютер або всю мережу трафіком, поки не відбудеться завершення роботи через перевантаження. DoS-атака також може блокувати трафік, що призводить до втрати доступу авторизованих користувачів до ресурсів мережі.
сніферська атака	Сніффер – це програма або пристрій, який може зчитувати, контролювати та фіксувати обмін даними в мережі та зчитувати мережеві пакети. Якщо пакети не зашифровані, сніффер забезпечує повний перегляд даних усередині пакета. Навіть інкапсульовані (тунельовані) пакети можна зламати та прочитати, якщо вони не зашифровані, а суб'єкт загрози не має доступу до ключа

Усі перелічені вище категорії атак, можуть бути використані для нанесення шкоди компаніям, які є ціллю інсайдерів.

1.2 Методи виявлення інсайдерських атак та інструменти для захисту

Існує безліч методів та інструментів захисту від атак, нижче наведений список більш поширених, які використовують компанії задля свого захисту.

- **Контролювати дії користувача.** У журналі подій (Event Logging) можна переглядати дії користувачів та помітити підозрілі дії. Також можна скористатись Microsoft Security Event Log. Це допоможе відстежити події, які схожі на інсайдерські атаки).
- **Розмежувати контроль доступу.** Можна знизити ризик атак, правильно розподіливши права доступу, наприклад через групові політики в Active Directory.
- **Використовувати антивірусне програмне забезпечення, EDR-системи тощо.** Це допоможе знайти та заблокувати шкідливе програмне забезпечення.
- **Моніторити трафік мережі.** Можна знайти підозрілу активність у мережі, що допоможе знайти атаки на ранніх етапах. Для моніторингу мережі можна використати протокол NetFlow, який був розроблений компанією Cisco.
- **Зашифрувати дані.** Це допоможе захистити дані від несанкціонованого доступу.
- **Міжмережеві екрани(firewalls).** Потрібні для блокування атак з зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise Firewall TM та інші). Вони керують проходженням мережевого трафіку відповідно до правил (policies) захисту.
- **Засоби створення віртуальних приватних мереж VPN (Virtual Private Network).** Використовуються для організації захищених каналів передачі даних через незахищене середовище. Технології VPN забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування.

Після створення моделі загроз, організації зосереджуються на виявленні та усуненні внутрішніх загроз і порушень безпеки.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Команди безпеки повинні розрізняти звичайну активність користувача та потенційно зловмисну активність, щоб виявити внутрішні загрози. Щоб розмежувати види діяльності, організації повинні спочатку усунути прогалини у видимості. Потім вони повинні агрегувати дані безпеки в централізоване рішення для моніторингу, незалежно від того, чи є воно частиною платформи безпеки та керування подіями (SIEM) або автономного рішення аналітики поведінки користувачів і об'єктів (UEBA). Багато команд починають із журналів доступу, автентифікації та змін облікового запису. Потім вони розширюють сферу застосування до додаткових джерел даних, таких як віртуальна приватна мережа (VPN) і журнали кінцевих точок, у міру того, як розвиваються випадки використання інсайдерської загрози.

Організації повинні прийняти рішення для керування привілейованим доступом (PAM) і передавати дані про доступ до привілейованих облікових записів із цього рішення до своєї SIEM. Коли організації централізують інформацію, вони зможуть моделювати поведінку користувачів і призначати оцінки ризику. Оцінки ризику прив'язані до певних ризикованих подій, таких як зміна географії користувача або завантаження на знімний носій. Призначення оцінок ризику також дає командам центру безпеки (SOC) можливість відстежувати ризики в масштабах підприємства, створюючи списки спостереження або виділяючи найбільш ризикованих користувачів у своїй організації.

Завдяки орієнтованому на користувача погляду служби безпеки можуть швидко виявляти внутрішню загрозу та керувати ризиками користувача з централізованого місця. Наприклад, аналітика поведінки користувачів може виявляти незвичайні спроби входу в незвичайний час доби або з незвичайного місця, або численні невдалі спроби ввести пароль, і створювати відповідне сповіщення для перевірки аналітиком. Іншими словами, будь-які аномалії поведінки допоможуть визначити, коли користувач став зловмисним інсайдером або якщо зовнішній зловмисник скомпрометував його облікові дані.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

Після перевірки система безпеки, автоматизації та реагування (SOAR) може створити робочий процес усунення внутрішніх загроз. Потенційне виправлення може включати звернення до інсайдера з MFA або скасування доступу, будь-яке з яких може бути виконано автоматично в рішенні для керування доступом до ідентифікаційної інформації (IAM).

1.3 Вразливості мережі на базі Windows

Мережі на базі Windows мають різні вразливості, які можуть бути використані для атак зовнішніх або інсайдерських атак. Найбільш поширені вразливості мереж на базі Windows включають наступні різновиди.

- Вразливості в протоколах мережі, а саме: SMB, RDP і DNS. Вони можуть бути використані для атак з-за кордону.
- Вразливості в службах мережі, а саме: служба друку, служба планування завдань і служба керування даними. Вони можуть бути використані для отримання несанкціонованого доступу до системи.
- Вразливості в програмному забезпеченні, а саме: браузері, поштові клієнти і медіа-програвачі. Вони можуть бути використані для розповсюдження шкідливих програм на комп'ютерах мережі.

Як наслідок компанія може отримати такі ризики:

- пошкоджені дані;
- несанкціонований доступ до даних компанії;
- втрата грошей;
- різні види атак(спам-атаки, фішинг, соціальна інженерія).

Висновки до першого розділу

У першому розділі було проаналізовано мотивацію порушників, види інсайдерських атак. Було розглянуто методи виявлення атак, наприклад: розмежування прав доступу та інші. Також було розглянуто основні вразливості на базі Windows.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ ВІД ІНСАЙДЕРСЬКИХ АТАК WINDOWS-МЕРЕЖІ

2.1 Вибір обладнання для організації роботи мережі

При виборі обладнання для організації роботи мережі потрібно врахувати, щоб воно містило достатню кількість портів та підтримувало всі необхідні технології та стандарти.

2.1.1. Вибір маршрутизаторів

Серія маршрутизаторів Cisco 7200, також відома як Cisco 7200 Series Router, є групою маршрутизаторів, розроблених компанією Cisco Systems. Ці маршрутизатори є одними з найпотужніших і гнучких пристроїв у лінійці Cisco[5].

Cisco 7200 Series Router забезпечує високу продуктивність, надійність та масштабованість для великих корпоративних мереж та провайдерів послуг. Вони використовуються для маршрутизації і комутації даних у мережах з високою пропускну здатністю.

Основні особливості серії маршрутизаторів Cisco 7200 включають наступні.

1. Висока продуктивність: Cisco 7200 може обробляти великий обсяг трафіку і виконувати складні функції маршрутизації без затримок і втрати швидкості передачі даних. Маршрутизатор може досягати швидкості обробки до 2 мільйонів пакетів за секунду (pps) і маю пропускну здатність до 1,4 Тбіт/с.

2. Гнучкість: Ці маршрутизатори підтримують різноманітні інтерфейси, включаючи Ethernet, Fast Ethernet, Gigabit Ethernet, ATM, T1/E1 і інші. Це дозволяє підключати їх до різних типів мереж і пристроїв.

3. Масштабованість: Cisco 7200 може бути розширений за допомогою модулів і інтерфейсів розширення, що дозволяє збільшити його можливості і пропускну здатність. Вони також підтримують багаторівненву комутацію і можуть обробляти велику кількість маршрутів.

4. Надійність: Cisco 7200 має вбудовані механізми захисту, такі як відновлення після збою, механізми забезпечення доступності та інші функції для забезпечення неперервної роботи мережі. Маршрутизатори Cisco 7200 підтримують різні

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

механізми захисту, включаючи файрвол, VPN, IPSec, аутентифікацію користувачів, контроль доступу до мережі (ACL) та інші функції безпеки.

5. Розширюваність: Ці маршрутизатори можуть працювати з різними оперативними системами Cisco IOS, що дозволяє налаштувати їх під конкретні потреби мережі.

Cisco 7200 Series Router є потужним і надійним рішенням для побудови складних мереж з високою пропускнуою здатністю. Вони дозволяють організаціям ефективно керувати мережею та забезпечувати якісне обслуговування користувачів.



Рисунок 2.1 Маршрутизатор Cisco 7200 Series VXR

2.1.2. Вибір комутаторів

Для організації комутації було обрано комутатор Cisco 2960, що дозволяє організувати розвинену та надійну локальну мережу не лише у великих компаніях та корпораціях, а й у системі філій. Надійна зафіксована конфігурація Cisco 2960 забезпечує мережеве підключення на швидкостях від 10 до 100 Мбс. Серед інших переваг C2960 можна виділити такі технічні характеристики, як:

- можливість підключення Fast та Gigabit Ethernet у версіях з 8 портів, 24 порти та 48 портів;

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

- можливість передачі електроживлення через кручену пару у версії з 24 портами;
- посилені функції забезпечення безпеки, а саме створення складних списків управління доступу;
- широкий спектр варіантів керування якістю обслуговування;
- інтелектуальна сервісна система на межі мережі;
- гарантійне обслуговування протягом терміну придатності обладнання.
- кожен комутатор має у комплекті ПЗ - Cisco Network Assistant. Це програмне забезпечення дозволяє налагодити структуроване керування всіма пристроями мережі, включає безліч майстрів автоматичного і ручного налаштування, що роблять процес налаштування та управління комутатором простим і надійним [6].



Рисунок 2.2 Cisco Catalyst 2960-24LC-S

2.2 Розробка моделі загроз для компанії

Перед створенням політики безпеки необхідно проаналізувати можливі загрози. Це дасть змогу оцінити усі можливі ризики та вберегти конфіденційні дані та інформацію компанії від потенційних загроз.

Модель загроз – це структуроване представлення всієї інформації, яка впливає на безпеку мережі. По суті, це погляд на програму та її середовище через призму безпеки [7].

Модель загроз повинна містити:

- потенційні загрози;
- дії, які можна вжити для пом'якшення або усунення кожної загрози;

Нижче описана схема моделі загроз для декількох рівнів.

На рівні фізичної безпеки, слід врахувати такі загрози.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- **Викрадення або втрата фізичних носіїв даних.** Втрата фізичних носіїв може призвести до втрати важливих даних, які можуть бути використані для шантажу або шкоди компанії. Це може статись через халатність працівників, зловживання владою, чи з метою завдати шкоди компанії, самим працівником.
- **Несанкціонований доступ до пристроїв.** Це може призвести до несправності пристроїв та небажаних дій зі сторони зловмисника. Це може статись через недотримання політик безпеки та недостатньої захищеності пристроїв.

Щоб пом'якшити чи усунути загрози на рівні фізичної безпеки, слід вживати наступні заходи.

- **Забезпечити безпеку обладнання.** Щоб захистити безпеку обладнання, потрібно надати доступ до кімнати з обладнання обмеженому колу осіб, зробити контроль доступу на дверях, який буде зчитувати чіп працівника та встановити відеоспостереження, наприклад з технологією розпізнаванням обличчя.
- **Зашифрувати фізичні носії даних.** Це забезпечить захист даних, які знаходяться на фізичних носіях (жорсткі диски, флеш-накопичувачі, DVD-диски і т.д.).

На рівні мережевої безпеки, слід врахувати такі загрози.

- **Атака Man-in-the-middle (рис. 2.3.).** Метою атаки є викрадення особистої інформації, такої як облікові дані, дані облікового запису та номери кредитних карток. Інформація, отримана під час атаки, може бути використана для багатьох цілей, включаючи крадіжку особистих даних, несхвалені перекази коштів або незаконну зміну пароля [8]. Цей вид атаки може використовуватись для атаки модифікації даних (табл. 1.1). Це може статись через недостатню захищеність мережі, використання незахищених протоколів чи вразливостей у програмному забезпеченні.
- **Атака DoS (Denial-of-Service).** Зловмисники DoS використовують уразливість програмного забезпечення в системі та продовжують виснажувати

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

оперативну пам'ять або центральний процесор сервера. Це може призвести до втрати даних, фінансовим втратам та відмові у доступі до сервісів.

Щоб пом'якшити чи усунути загрози на рівні мережевої безпеки, слід вжити наступні заходи.

- **Використовувати Firewall.** Це допоможе блокувати небажаний чи шкідливий трафік з Інтернету та захистить мережу від зовнішніх атак.
- **Шифрувати дані.** Це забезпечить надійне передавання конфіденційної інформації. Необхідно налаштувати протоколи, які шифрують дані, такі як: IPsec, SSH чи PGP.
- **Встановити міцні паролі.** Це можна зробити за допомогою групової політики у Active Directory.
- **Навчання працівників.** Створити курс для працівників, який ознайомить працівників із засобами безпеки, розпізнавати фішингові та інші атаки.
- **Моніторинг.** Необхідно встановити систему моніторингу мережі для виявлення вторгнень. Це допоможе швидко виявляти потенційні загрози та швидко відреагувати на загрози.

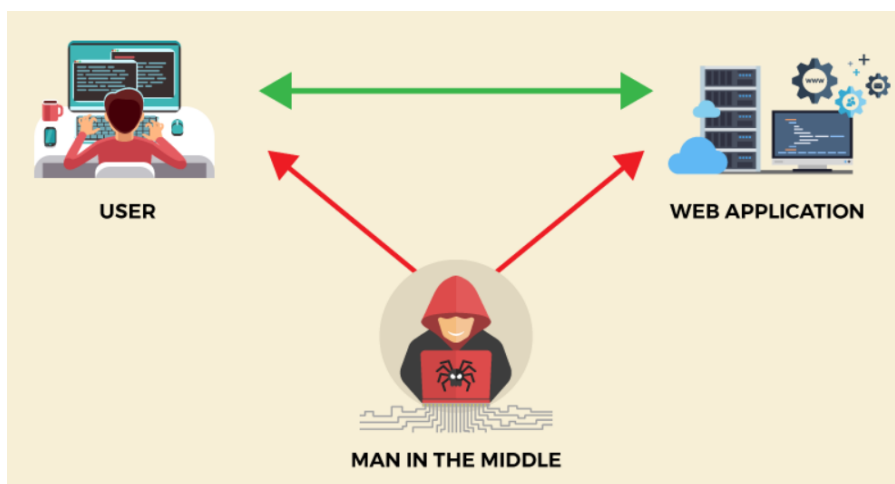


Рисунок 2.3 – Демонстрація атаки Man in the middle

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

2.3 Розробка політики безпеки для співробітників

Розробка політики безпеки компанії є невід'ємною частиною захисту мережі. Тому, кожен новий працівник перед початком роботи має ознайомитись з політикою безпеки.

Для запобігання отримання вірусу на ПЗ чи можливості надання шкоди компанії, вирішено обмежити права на користування ПК та заборонити деякі дії.

Зокрема, користувачам заборонено:

- 1) Самостійно встановлювати програми
- 2) Модифікувати встановлене програмне забезпечення
- 3) Самостійно перевстановлювати ПЗ
- 4) Самостійно видаляти ПЗ
- 5) Використовувати флеш-носій не перевіривши його на вірус
- 6) Використовувати стороннє програмне забезпечення
- 7) Використовувати ПЗ для цілей, які не пов'язані з виробничою діяльністю та з виконанням посадових обов'язків
- 8) Використовувати один обліковий запис для декількох працівників

Під час звільнення працівника, його обліковий запис блокується в день звільнення відповідно до наказу підприємства.

Правила, яких працівник має дотримуватись при виборі пароля:

- 1) Довжина пароля повинна складати не менше 8 символів
- 2) Забороняється використовувати назву облікового запису, ім'я або прізвище
- 3) Необхідно використовувати комбінацію з малих та великих латинських літер, цифр та інших символів

Також, потрібно змінювати пароль кожних 3 місяці, не записувати його будь-де та використовувати Кеерер для управління та збереження паролів від веб-сайтів і т. д.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Розробка проєкту мережі

Дана мережа була створена з 5 маршрутизаторів, 3 комутаторів, 12 робочих станцій та з серверу з Active Directory. В даній мережі було налаштовано протоколи OSPF та EIGRP, SSH.

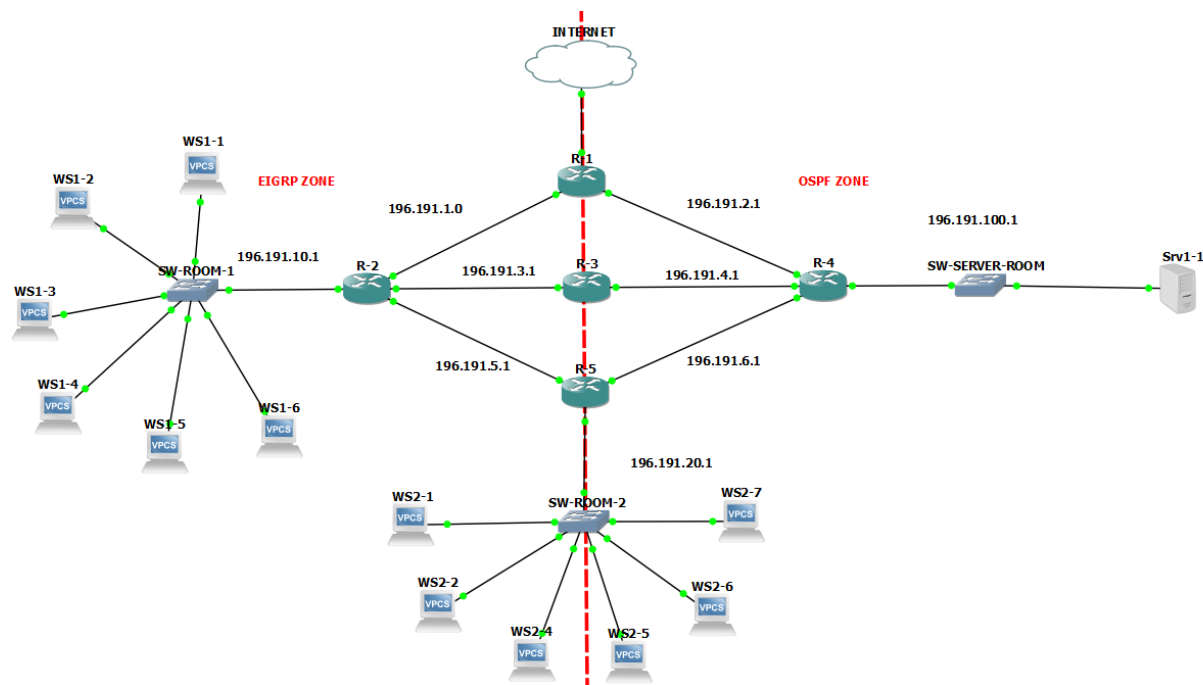


Рисунок 2.4 – Проєкт мережі

Розробка схеми адресації мережі

Нижче наведена таблиця адресації, яка була створена для модельованої мережі.

Таблиця 2.1 - Параметри IP-адресації мережі

Пристрій/ Підмережа	Інтерфейс/ Шлюз	IP-адреса	Маска	Преф.
Мережа Інтернет	-	192.198.122.0	255.255.255.0	/24
Cloud	Інтерфейс Virbr0	192.198.122.1	255.255.255.0	/24
R-1	Інтерфейс Fa0/0	192.198.122.101	255.255.255.0	/24
Мережа А	-	196.191.1.0	255.255.255.252	/30
R-1	Інтерфейс Fa1/0	196.191.1.1	255.255.255.252	/30
R-2	Інтерфейс Fa1/0	196.191.1.2	255.255.255.252	/30
Мережа В	-	196.191.2.0	255.255.255.252	/30
R-1	Інтерфейс Fa1/1	196.191.2.1	255.255.255.252	/30
R-4	Інтерфейс Fa1/1	196.191.2.2	255.255.255.252	/30
Мережа С	-	196.191.3.0	255.255.255.252	/30
R-3	Інтерфейс Fa0/0	196.191.3.1	255.255.255.252	/30

Пристрій/ Підмережа	Інтерфейс/ Шлюз	ІР-адреса	Маска	Преф.
R-2	Інтерфейс Fa0/0	196.191.3.2	255.255.255.252	/30
Мережа D	-	196.191.4.0	255.255.255.252	/30
R-3	Інтерфейс Fa0/1	196.191.4.1	255.255.255.252	/30
R-4	Інтерфейс Fa0/1	196.191.4.2	255.255.255.252	/30
Мережа E	-	196.191.5.0	255.255.255.252	/30
R-5	Інтерфейс Fa1/1	196.191.5.1	255.255.255.252	/30
R-2	Інтерфейс Fa1/1	196.191.5.2	255.255.255.252	/30
Мережа F	-	196.191.6.0	255.255.255.252	/30
R-5	Інтерфейс Fa1/0	196.191.6.1	255.255.255.252	/30
R-4	Інтерфейс Fa1/0	196.191.6.2	255.255.255.252	/30
Мережа G	-	196.191.10.0	255.255.255.0	/24
R-2	E2/0	196.191.10.1	255.255.255.0	/24
SW-ROOM-1	Vlan 10	196.191.10.2	255.255.255.0	/24
	Шлюз по замовчуванню	196.191.10.1	-	-
	Основний DNS- сервер	196.191.100.3	-	-
Робочі станції	Vlan 10	196.191.10.3 – 196.191.10.8	255.255.255.0	/24
	Шлюз по замовчуванню	196.191.10.1	-	-
	Основний DNS- сервер	196.191.100.3	-	-
Мережа H	-	196.191.20.0	255.255.255.0	/24
R-5	E2/0	196.191.20.1	255.255.255.0	/24
SW-ROOM-2	Vlan 20	196.191.20.2	255.255.255.0	/24
	Шлюз по замовчуванню	196.191.20.1	-	-
	Основний DNS- сервер	196.191.100.3	-	-
Робочі станції	Vlan 20	196.191.20.3 – 196.191.20.8	255.255.255.0	/24
	Шлюз по замовчуванню	196.191.20.1	-	-
	Основний DNS- сервер	196.191.100.3	-	-

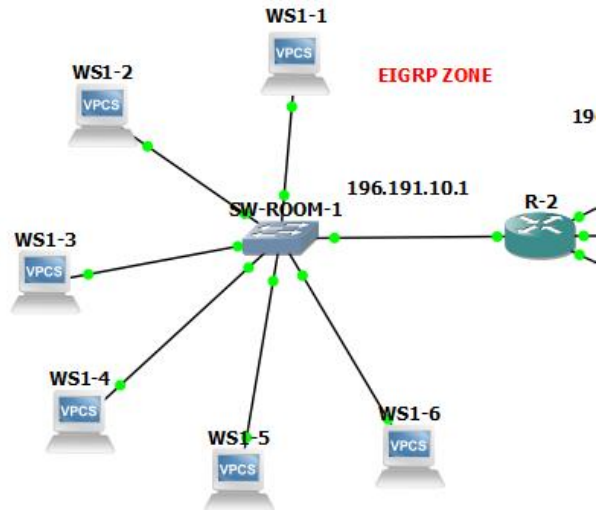


Рисунок 2.5 – Підмережа з VLAN 10

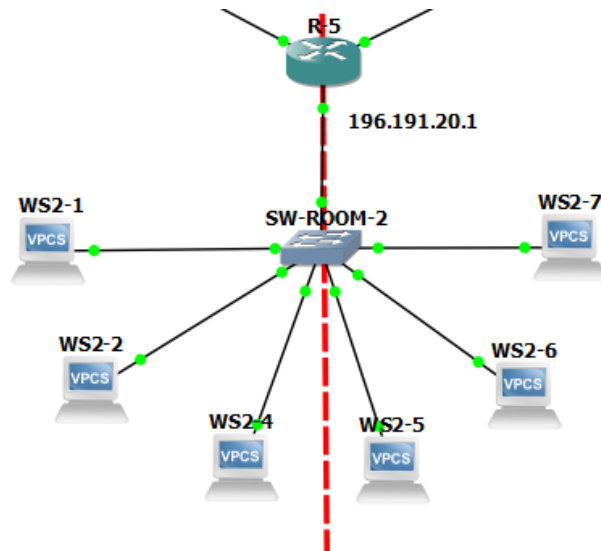


Рисунок 2.6 – Підмережа з VLAN 20

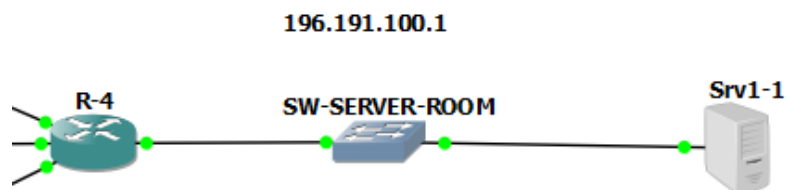


Рисунок 2.7 – Підмережа з VLAN 100

Повну топологію наведено у додатку.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

2.4 Відомості про OSPF та EIGRP

Одним із способів, за допомогою якого OSPF і EIGRP можуть допомогти захистити мережу від інсайдерів, є використання автентифікації між маршрутизаторами.

Обидва протоколи підтримують механізми автентифікації, такі як паролі та ключі. Це дозволяє маршрутизаторам перевіряти взаємну надійність перед тим, як обмінюватися інформацією про маршрутизацію. Якщо автентифікація невдається, маршрутизатор відмовляється спілкуватися з іншими маршрутизаторами, таким чином запобігаючи несанкціонованому доступу до мережі.

Порівняння протоколів EIGRP та OSPF. EIGRP заснований на DUAL (Diffusive Update Algorithm), тоді як OSPF використовує алгоритм SPF (Shortest Path First). Основна різниця між цими двома алгоритмами у тому, як вони обчислюють найкоротший шлях маршрутизації. SPF залежить тільки від пропускної здатності для розрахунку метрики, тоді як DUAL використовує пропускну здатність та затримку для обчислення складових метрик зі складними формулами.

Масштабованість OSPF краща, ніж EIGRP, тому що EIGRP більш складний у великих мережах при усуненні неполадок. Порівнянно з EIGRP, OSPF більше підходить для використання у глобальній мережі, оскільки більшість постачальників підтримують OSPF. OSPF вже працює у внутрішньому середовищі як IGP (Interior Gateway Protocol). Тому легко обмінюватися певними маршрутами з OSPF. Якщо використовувати інші протоколи маршрутизації та обмінюватися тією ж інформацією про маршрутизацію, маршрутизація стане складнішою, оскільки відбудеться перерозподіл між вбудованим протоколом OSPF та іншими протоколами.

OSPF зберігає інформацію про всі мережі та робочі маршрутизатори у своїй області. Щоразу, коли в області відбуваються зміни, всі маршрутизатори повинні повторно синхронізувати бази даних, а потім знову запускати SPF. Цей процес змушує CPU займати більше ресурсів. З іншого боку, EIGRP ініціює додаткові оновлення. Отже, з точки зору використання CPU, EIGRP ефективніший.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

EIGRP є популярним вибором для маршрутизації в малих та великих мережах. Коли мережеве обладнання постачається від різних постачальників, OSPF є найкращим вибором. OSPF також є найкращим вибором, оскільки він підтримує CSPF (Constrained Shortest Path First) для підтримки проектування трафіку MPLS.

Route redistribution

Поки не створено єдиний протокол маршрутизації, який керував би рештою, існує необхідність у тому, щоб кілька протоколів маршрутизації мирно співіснували в одній мережі. Наприклад, одна компанія працює з OSPF, а інша компанія працює з EIGRP і ці дві компанії злилися в одне підприємство.

Поки ІТ-персонал новоствореної компанії не перейде для використання на єдиний протокол маршрутизації, маршрути, відомі протоколу OSPF, необхідно оголосити в частину мережі, що працює під управлінням EIGRP, і навпаки. Це можливо завдяки Route redistribution – дозволяє мережі, що використовує один протокол маршрутизації, динамічно маршрутизувати трафік на основі інформації, отриманої з іншого протоколу маршрутизації.

Висновки до другого розділу

Була побудована мережа, яка включає в себе 5 маршрутизаторів, 3 комутатори, 12 робочих станцій та сервер з Active Directory, проаналізовано можливості вибраних пристроїв. Також була розроблена схема адресації мережі, розглянуто відомості про протоколи OSPF та EIGRP та складено політику безпеки для співробітників.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ WINDOWS-МЕРЕЖІ

3.1 Налаштування обладнання мережі

Для правильного функціонування мережі, потрібно налаштувати усі пристрої.

Сценарій налагодження протоколів EIGRP та OSPF на маршрутизаторах

```
R-1(config)#router eigrp 6
R-1(config-router)#net 196.191.1.0
R-1(config-router)#redistribute ospf 6 metric 100000 2 255 1 1500
R-1(config-router)#exit
R-1(config)#router ospf 6
R-1(config-router)#redistribute eigrp 6 subnets
R-1(config-router)#net 196.191.2.0 0.0.0.3 area 0
```

Рисунок 3.1 – Налаштування протоколів EIGRP та OSPF на маршрутизаторі R-1

```
R-2(config)#router eigrp 6
R-2(config-router)#net 196.191.1.0
R-2(config-router)#net 196.191.3.0
R-2(config-router)#net 196.191.5.0
R-2(config-router)#net 196.191.10.0
```

Рисунок 3.2 – Налаштування протоколів EIGRP на маршрутизаторі R-2

```
R-3(config)#router eigrp 6
R-3(config-router)#redistribute ospf 6 metric 100000 2 255 1 1500
R-3(config-router)#net 196.191.3.0
R-3(config-router)#router ospf 6
R-3(config-router)#redistribute eigrp 6 subnets
R-3(config-router)#net 196.191.4.0 0.0.0.3 area 0
```

Рисунок 3.3 – Налаштування протоколів EIGRP та OSPF на маршрутизаторі R-3

```
R-4(config)#router ospf 6
R-4(config-router)#net 196.191.2.0 0.0.0.3 area 0
R-4(config-router)#net 196.191.4.0 0.0.0.3 area 0
R-4(config-router)#net 196.191.6.0 0.0.0.3 area 0
R-4(config-router)#net 196.191.100.0 0.0.0.255 area 0
```

Рисунок 3.4 – Налаштування протоколів OSPF на маршрутизаторі R-4

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-5(config)#router eigrp 6
R-5(config-router)#redistribute ospf 6 metric 100000 2 255 1 1500
R-5(config-router)#net 196.191.5.0
R-5(config-router)#net 196.191.20.0
R-5(config-router)#router ospf 6
R-5(config-router)#redistribute eigrp 6 subnets
R-5(config-router)#net 196.191.6.0 0.0.0.3 area 0

```

Рисунок 3.5 – Налаштування протоколів EIGRP та OSPF на маршрутизаторі R-5

Далі наведено сценарій налаштування VLAN на пристроях:

VLAN 10

```

SW-ROOM-1(config)#vlan 10
SW-ROOM-1(config-vlan)#name ROOM-1
SW-ROOM-1(config-vlan)#exit
SW-ROOM-1(config)#int vlan 10
SW-ROOM-1(config-if)#ip add 196.191.10.2 255.255.255.0
SW-ROOM-1(config-if)#no sh
SW-ROOM-1(config-if)#exit
SW-ROOM-1(config)#int e0/1
SW-ROOM-1(config-if)#switchport mode acc
SW-ROOM-1(config-if)#switchport acc vlan 10
SW-ROOM-1(config-if)#exit
SW-ROOM-1(config)#int e0/0
SW-ROOM-1(config-if)#switchport trunk encapsulation dot1q
SW-ROOM-1(config-if)#switchport mode trunk
SW-ROOM-1(config-if)#ip default-gate 196.191.10.1

```

Рисунок 3.6 – Налаштування VLAN 10 на комутаторі SW-ROOM-1

VLAN 20

```

SW-ROOM-2(config)#vlan 10
SW-ROOM-2(config-vlan)#name ROOM-2
SW-ROOM-2(config-vlan)#exit
SW-ROOM-2(config)#int vlan 10
SW-ROOM-2(config-if)#ip add 196.191.20.2 255.255.255.0
SW-ROOM-2(config-if)#no sh
SW-ROOM-2(config-if)#exit
SW-ROOM-2(config)#int e0/1
SW-ROOM-2(config-if)#switchport mode acc
SW-ROOM-2(config-if)#switchport acc vlan 20
% Access VLAN does not exist. Creating vlan 20
SW-ROOM-2(config-if)#exit
SW-ROOM-2(config)#int e0/0
SW-ROOM-2(config-if)#switchport trunk encapsulation dot1q
SW-ROOM-2(config-if)#switchport mode trunk
SW-ROOM-2(config-if)#ip default-gate 196.191.20.1

```

Рисунок 3.7 – Налаштування VLAN 20 на комутаторі SW-ROOM-2

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

```

R-2(config)#int e2/0.20
R-2(config-subif)#encapsulation dot1q 20
R-2(config-subif)#ip add 196.191.20.1 255.255.255.0
R-2(config-subif)#no sh
R-2(config-subif)#exit
R-2(config)#int e2/0
R-2(config-if)#no sh
R-2(config-if)#exit

```

Рисунок 3.8 – Налаштування VLAN 20 на маршрутизаторі R-2

VLAN 100

```

SW-SERVER-ROOM(config)#int e0/1
SW-SERVER-ROOM(config-if)#switchport mode acc
SW-SERVER-ROOM(config-if)#switchport acc vlan 100
% Access VLAN does not exist. Creating vlan 100
SW-SERVER-ROOM(config-if)#no sh
SW-SERVER-ROOM(config-if)#exit
SW-SERVER-ROOM(config)#vlan 100
SW-SERVER-ROOM(config-vlan)#name SERVER-ROOM
SW-SERVER-ROOM(config-vlan)#exit
SW-SERVER-ROOM(config)#int vlan 100
SW-SERVER-ROOM(config-if)#ip add 196.191.100.2 255.255.255.0
SW-SERVER-ROOM(config-if)#no sh
SW-SERVER-ROOM(config-if)#exit
SW-SERVER-ROOM(config)#ip default-gateway 196.191.100.1

```

Рисунок 3.9 – Налаштування VLAN 100 на комутаторі SW-SERVER-ROOM

```

R-4(config)#int e2/0.100
R-4(config-subif)#encapsulation dot1q 100
R-4(config-subif)#ip add 196.191.100.1 255.255.255.0
R-4(config-subif)#no sh
R-4(config-subif)#exit
R-4(config)#int e2/0
R-4(config-if)#no sh
R-4(config-if)#exit

```

Рисунок 3.10 – Налаштування VLAN 100 на маршрутизаторі R-4

Також було налаштовано протокол віддаленого доступу SSH.

SSH (Secure Shell) – тип мережевого протоколу, який шифрує паролі та передану інформацію, прикладний протокол SSH був представлений в 1995 році, але через деякі вразливості в 1996 році була розроблена друга версія. До цього дня всі

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

користуються стандартом SSH, який залишається незмінним вже багато-багато років і гарантує безпечну передачу даних [4].

Приклад налаштування SSH на маршрутизаторі R-1. На інших пристроях були проведені аналогічні налаштування.

```
R-1(config)#ip domain name yesypenko.net
R-1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: R-1.yesypenko.net

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 36 seconds)

R-1(config)#service password-encryption
R-1(config)#username admin privilege 15 secret Cisco1234
R-1(config)#enable secret Cisco1234
R-1(config)#line vty 0 4
R-1(config-line)#transport input ssh
R-1(config-line)#transport output ssh
R-1(config-line)#exec-timeout 60 0
R-1(config-line)#exit
```

Рисунок 3.11 – Налаштування SSH на маршрутизаторі R-1

3.2 Налаштування Active Directory на базі Windows Server 2019

Після успішного налаштування мережі, приступимо до налаштування Active Directory.

Приклад додавання робочих станцій з різних VLAN до домену показано на рис. 3.1-3.4.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

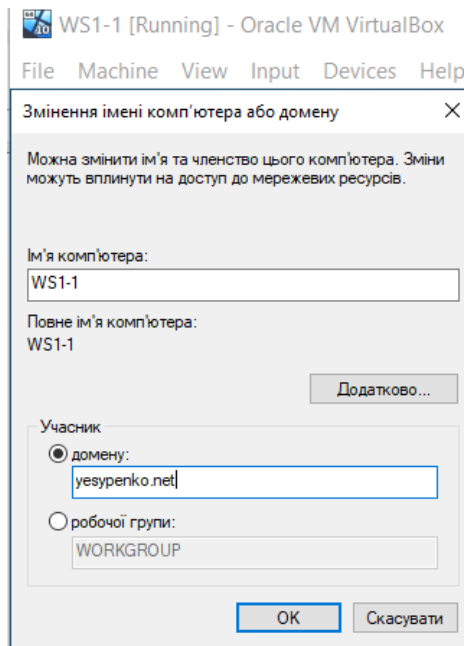


Рисунок 3.12 – Під'єднання комп'ютера WS1-1(WLAN 10) до домену
yesypenko.net

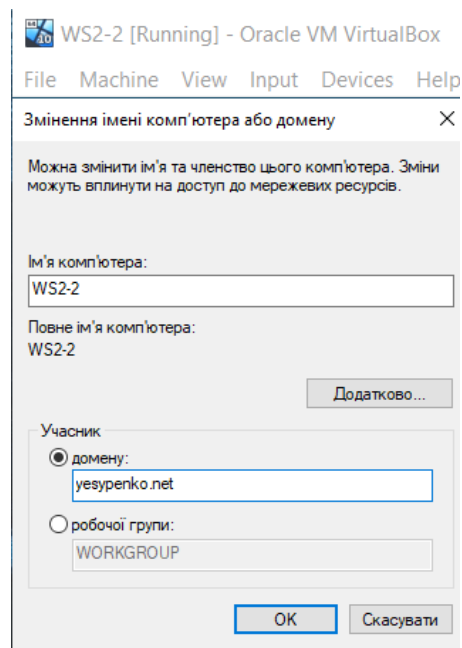


Рисунок 3.13 – Під'єднання комп'ютера WS2-1(WLAN 20) до домену
yesypenko.net

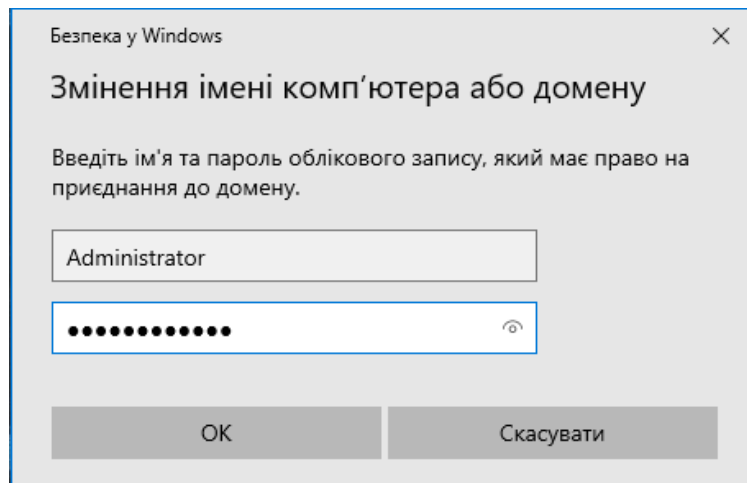


Рисунок 3.14 – Введення даних запису з правами на підключення

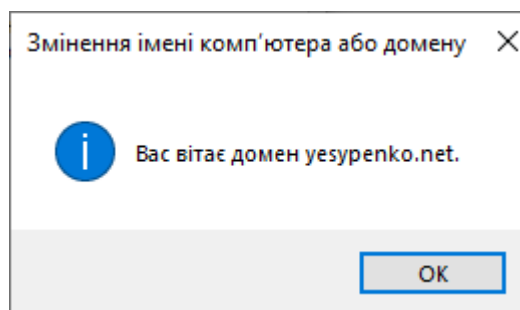


Рисунок 3.15 – Результат успішного приєднання комп'ютерів

Також це можна перевірити і на самому сервері.

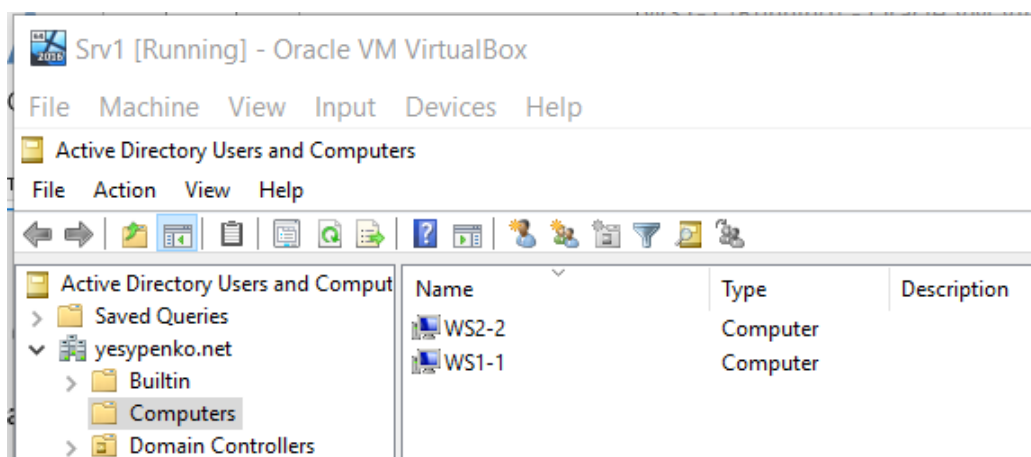


Рисунок 3.16 – Перевірка приєднання ПК на сервері

Тепер необхідно створити облікові записи для користувачів. Нижче наведено поетапний приклад створення.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Заповнюємо усі необхідні поля(рис. 3.17)

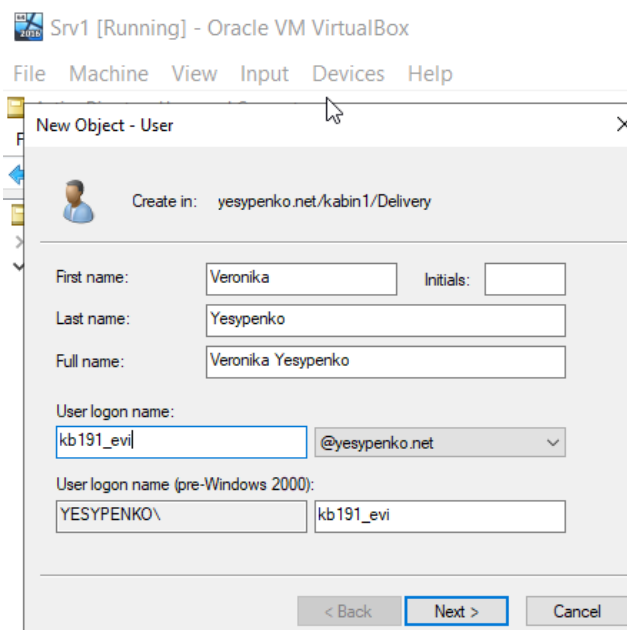


Рисунок 3.17 – Налаштування основних полів при створенні нового користувача

2. Далі задамо пароль та поставимо галочку, щоб користувач змінив пароль при першому вході(рис. 3.18-3.19).

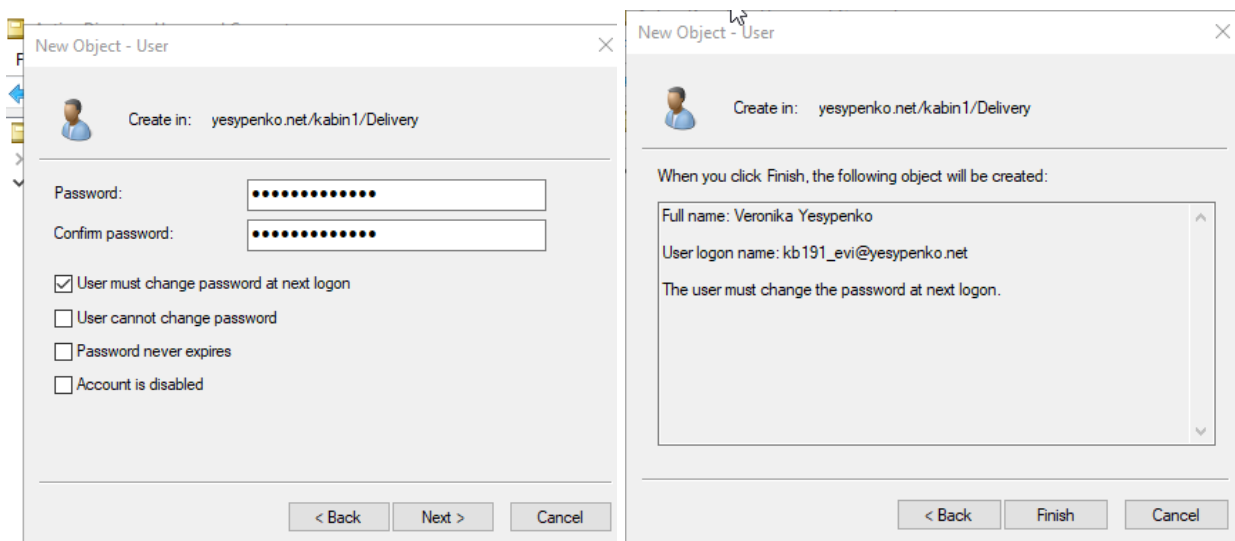


Рисунок 3.18-3.19 – Задання паролю та інформація про користувача якого буде створено

Аналогічно створюємо й інших користувачів, які відносяться до різних департаментів.

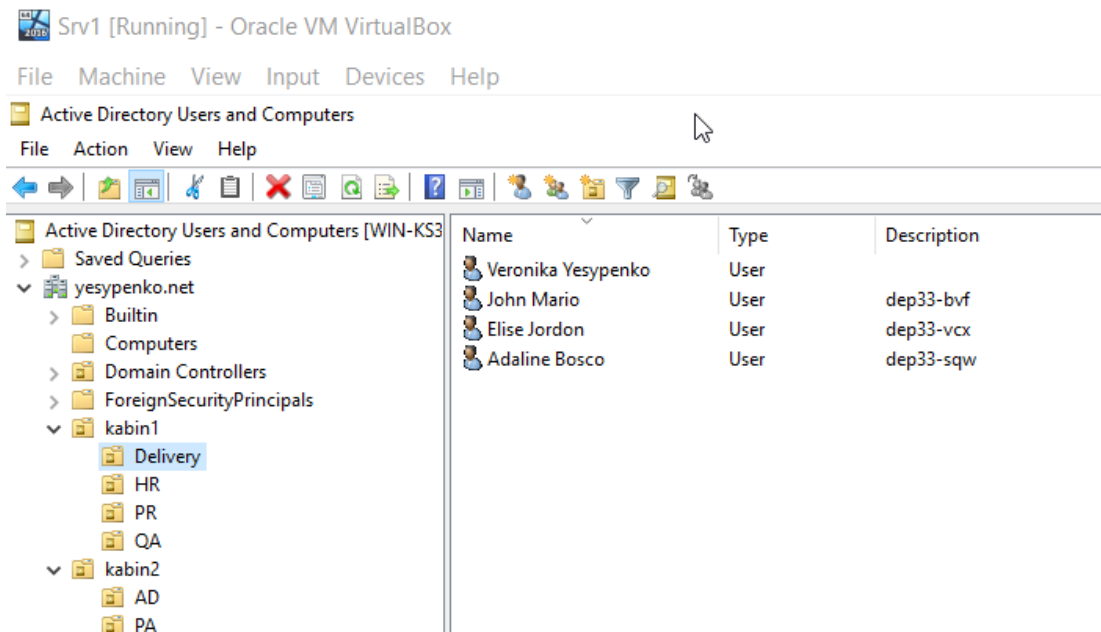


Рисунок 3.20 – Результат створення користувачів

Наступним кроком є створення політики для користувачів. Це необхідно для захисту інформації, яка буде міститись на ПК.

Налаштування блокування облікового запису після 3 невдалих спроб входу продемонстровано на рис. 3.21.

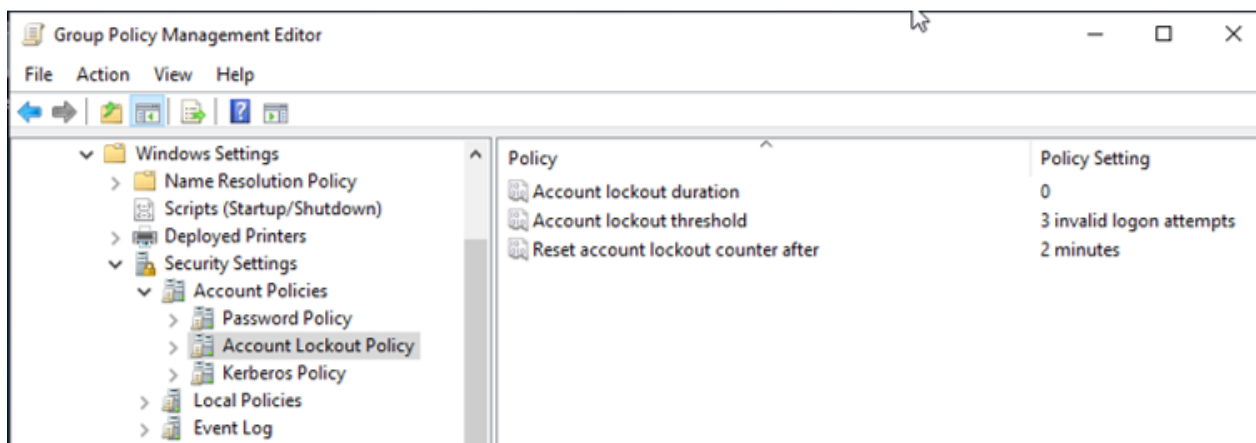


Рисунок 3.21 – Налаштування Account Lockout Policy об'єкта групової політики Default Domain Policy

Також потрібно заборонити встановлювати програми без відома адміністратора (рис. 3.22)[1].

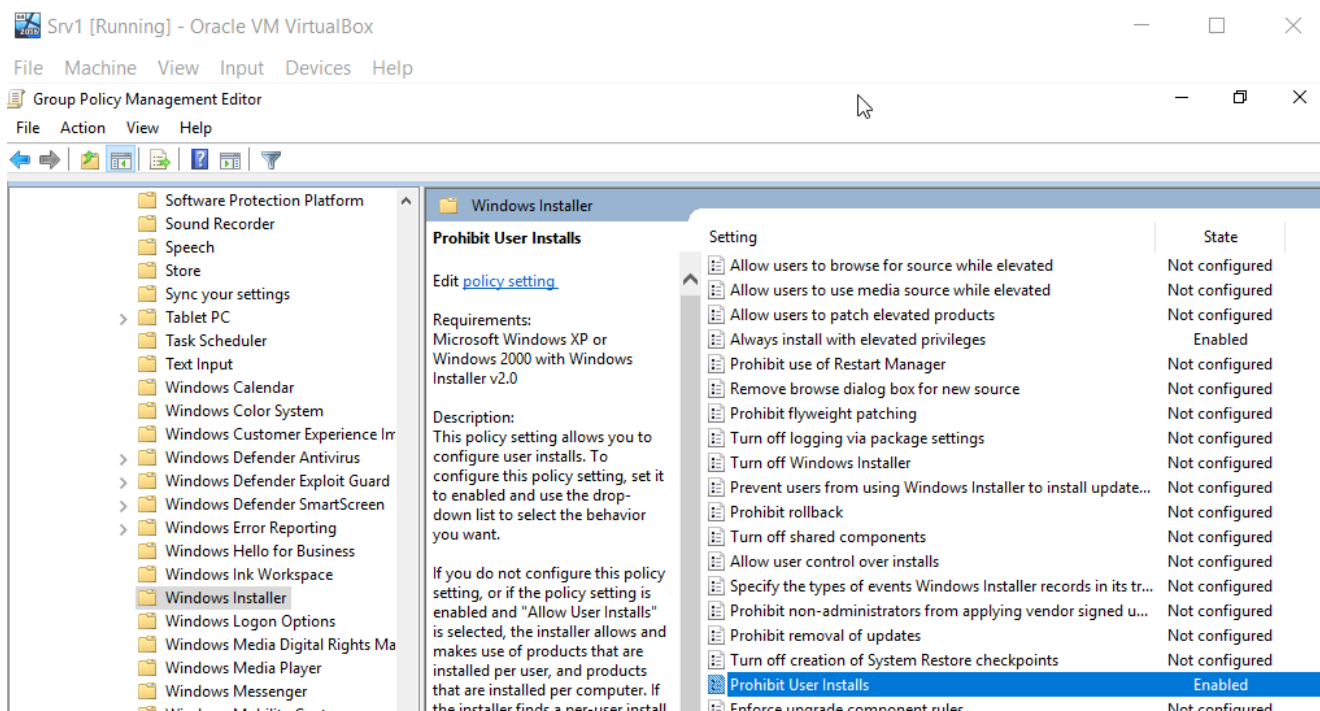


Рисунок 3.22 – Заборона встановлювати програми

Забороняємо доступ до панелі керування

Користувачі можуть вносити значні зміни в налаштування системи за допомогою панелі керування, і ці зміни можуть призвести до проблем із безпекою. Для безпечнішого бізнес-середовища обмежимо доступ до панелі керування лише для привілейованих користувачів[1].

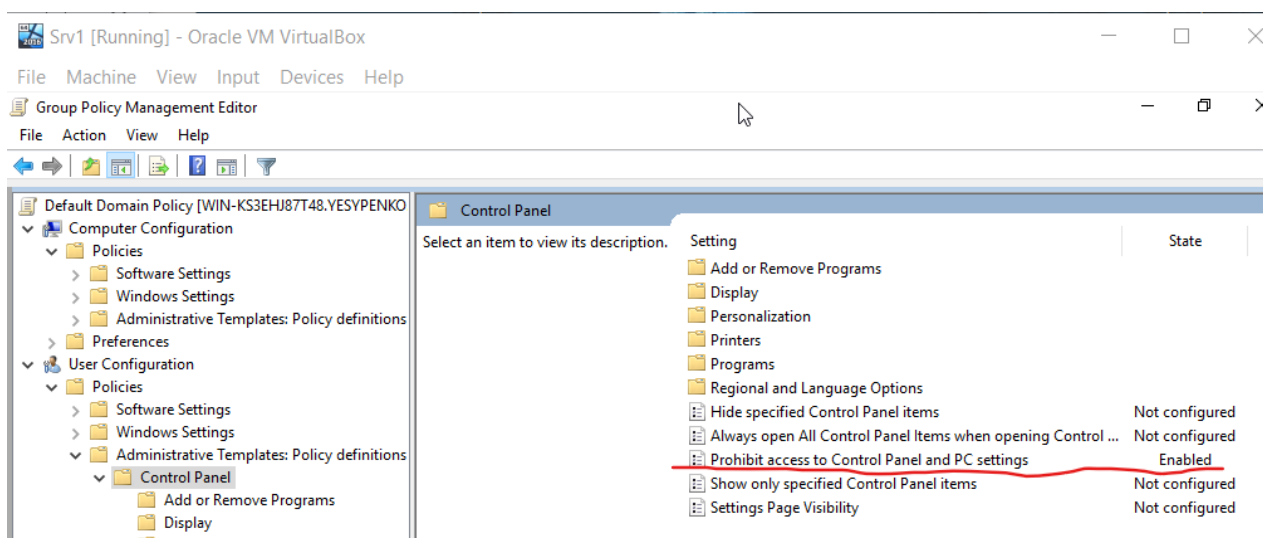


Рисунок 3.23 – Заборонений доступ до «Панелі керування»

Забороняємо доступ до командного рядка (рис. 3.24).

Командний рядок у Windows використовується для запуску команд, які виконують розширені адміністративні функції. Однак у руках зломисників командний рядок може використовуватися для порушення цілісності системи[1].

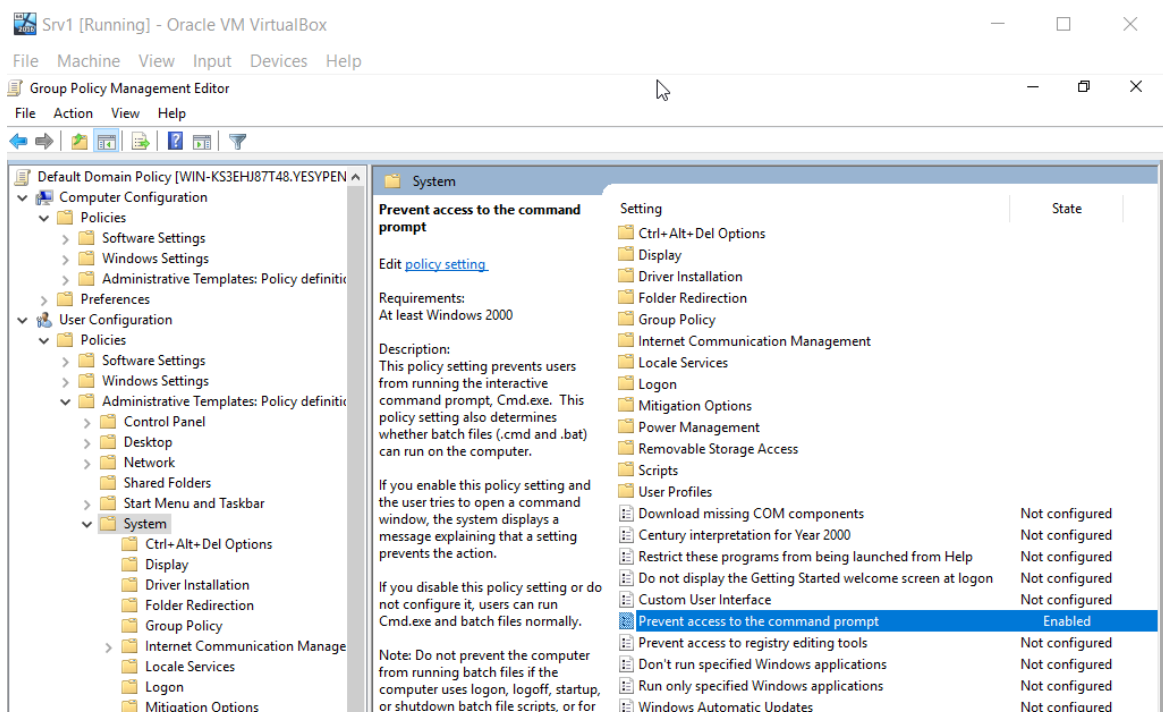


Рисунок 3.24 – Заборонений доступ до «Командний рядок»

Далі необхідно налаштувати політику для паролів, яка буде відповідати усім правилам безпеки (рис. 3.25).

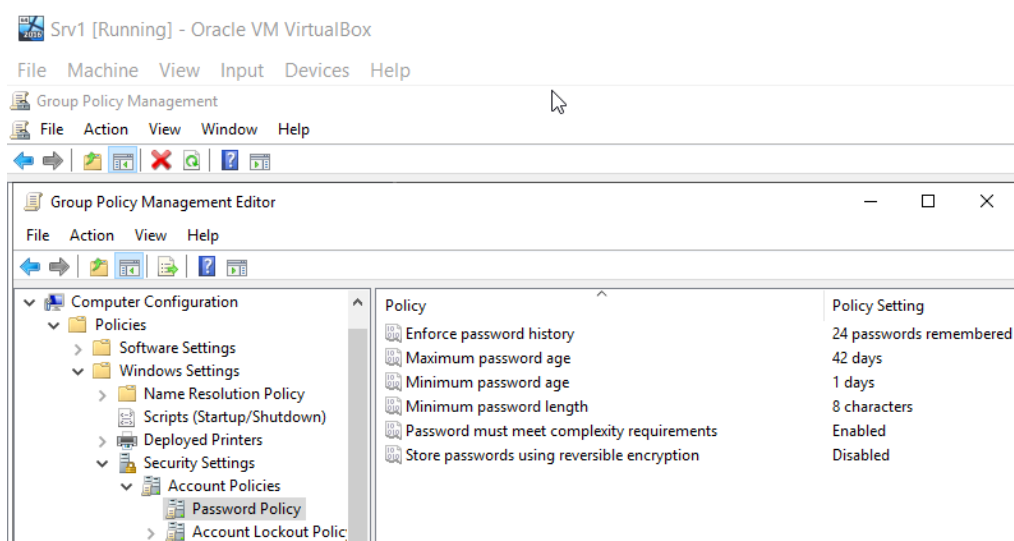


Рисунок 3.25 – Налаштування політики паролів

Забороняємо доступ до всіх знімних накопичувачів

Знімні пристрої вразливі до вірусів і зловмисного програмного забезпечення, і якщо користувачі зможуть підключити їх до своїх комп'ютерів, це може заразити всю мережу. Знімні пристрої також дозволяють зловмисникам видаляти великі обсяги даних за короткий час.

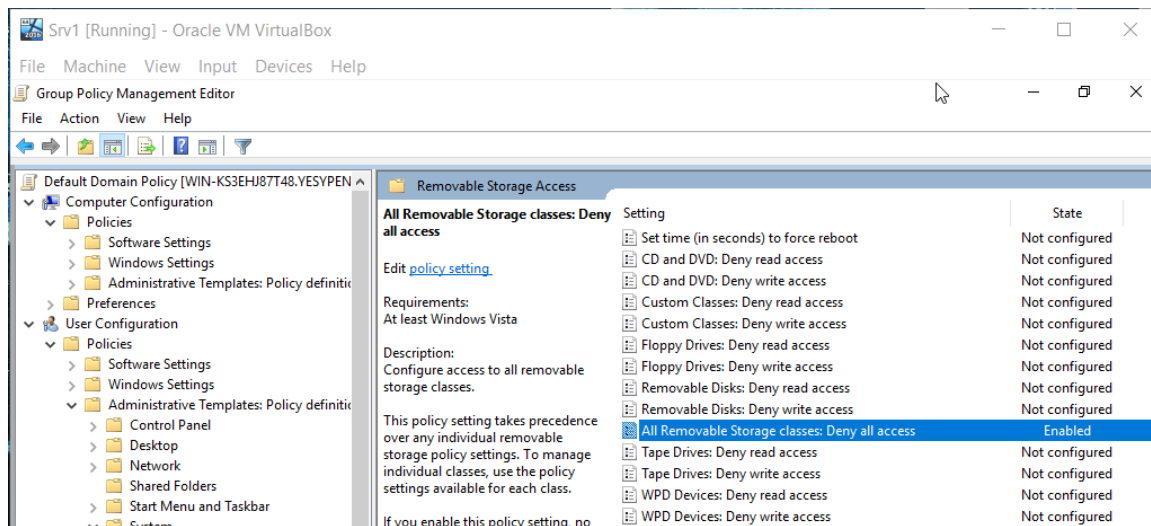


Рисунок 3.26 – Заборонений доступ до всіх знімних накопичувачів

Заборона зберігання хеш-значення LAN Manager під час наступної зміни пароля продемонстрована на рис. 3.27.

Windows зберігає хеші паролів LAN Manager (LM) у локальній базі даних Security Accounts Manager (SAM). Ці хеші LM слабкі, і зловмисники можуть легко розшифрувати їх у формат відкритого тексту.

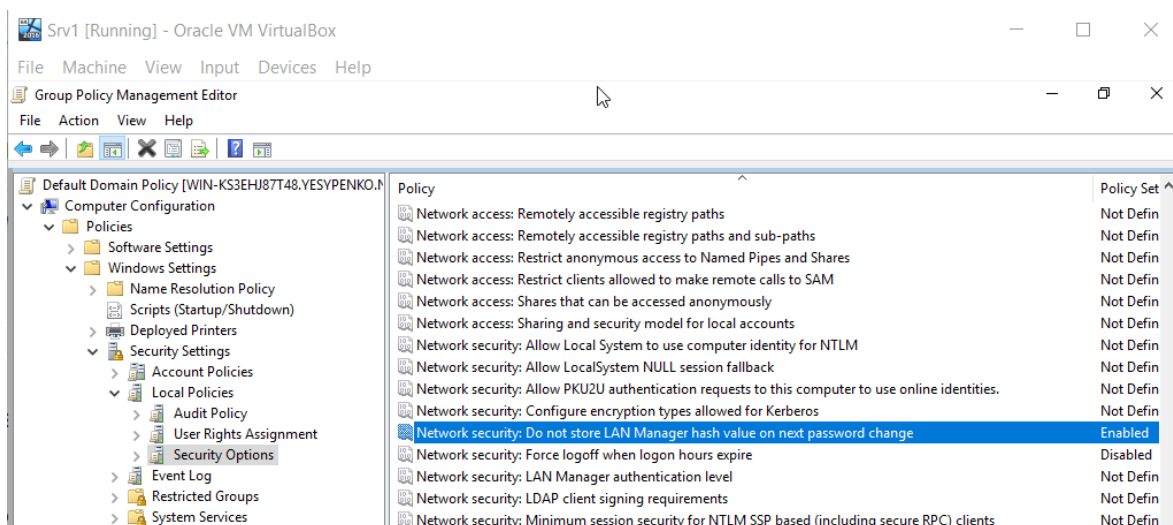


Рисунок 3.27 – Заборона зберігання хеш-значення LAN Manager

Після цього потрібно налаштувати політику аудиту подій входу та виходу в систему (рис.3.28-3.29). Це дає адміністратором можливість відстежувати усі сеанси входу.

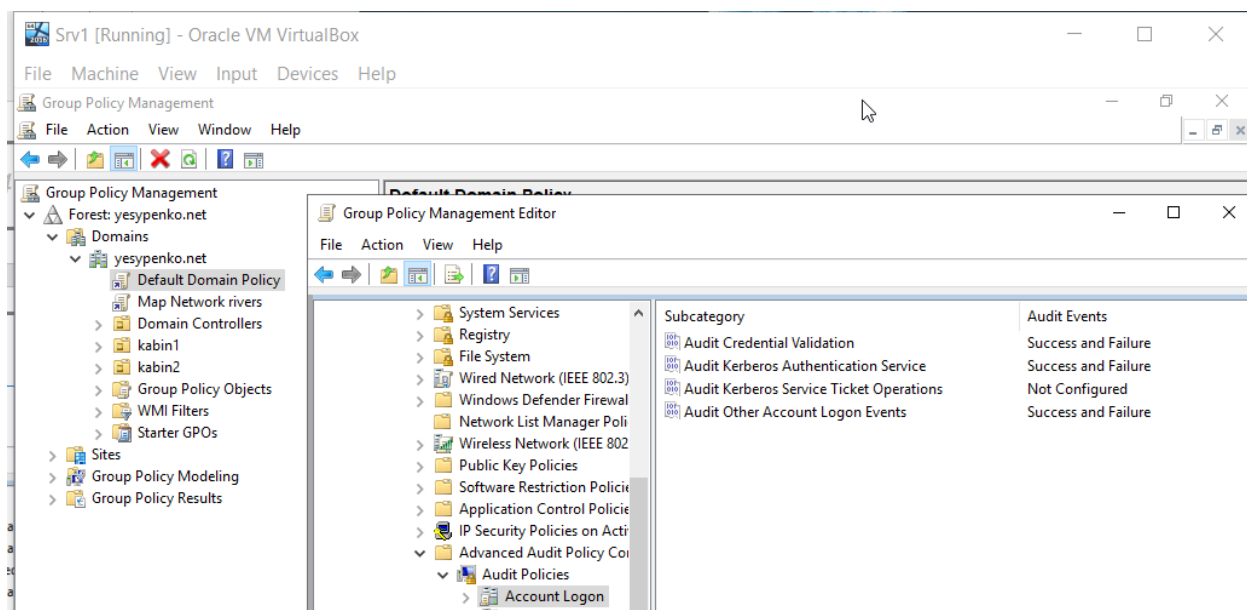


Рисунок 3.28 – Налаштування політики аудиту подій входу та виходу

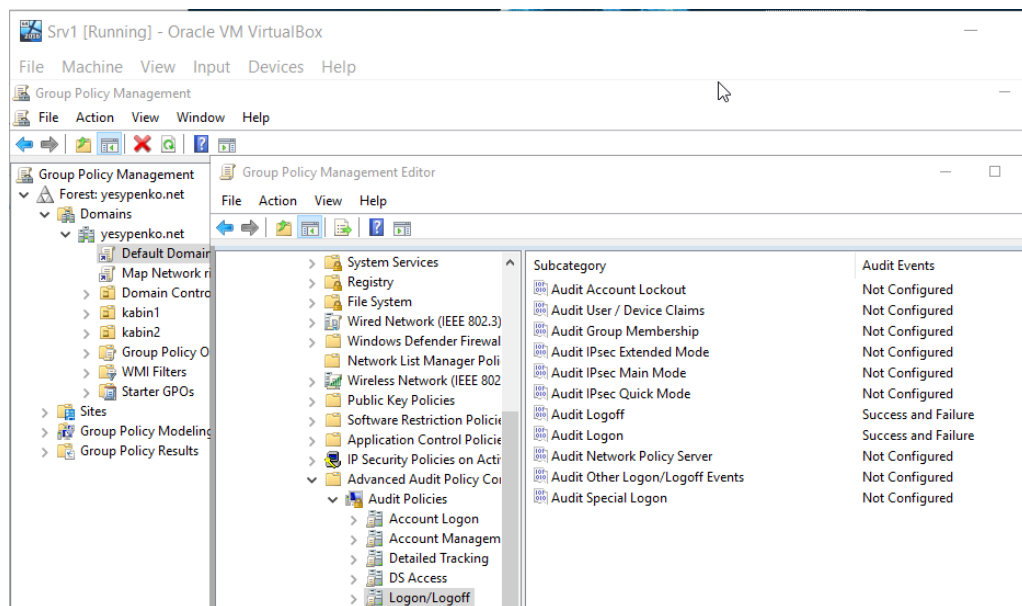


Рисунок 3.29 – Налаштування політики аудиту подій входу та виходу

Також здійснюємо налаштування політики аудиту доступу до об'єктів (рис.3.30).

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

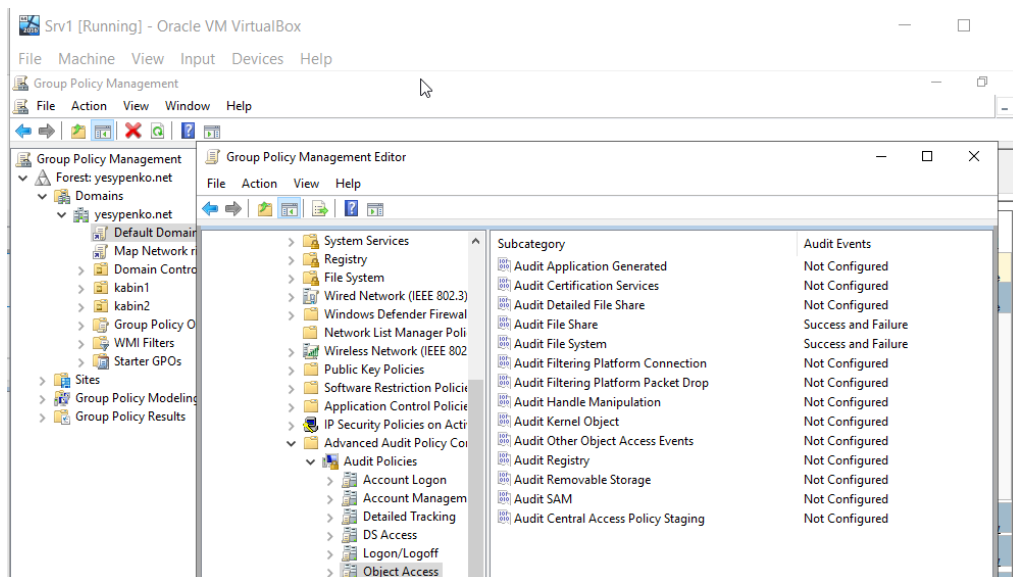


Рисунок 3.30 – Налаштування політики аудиту доступу до об’єктів

Також необхідно зашифрувати жорсткий диск. Це забезпечить захист даних, які знаходяться на фізичних носіях у разі викрадення.

Для робочих станцій з Windows 10 ми можемо налаштувати шифрування жорсткого диску через BitLocker.

Етапи увімкнення BitLocker:

1. на сервері дозволяємо використання BitLocker;
2. на сервері вмикаємо функцію збереження відновлювальної інформації на Active Directory (рис. 3.31-3.32);
3. створити пароль для розблокування;
4. почати шифрування жорсткого диску;

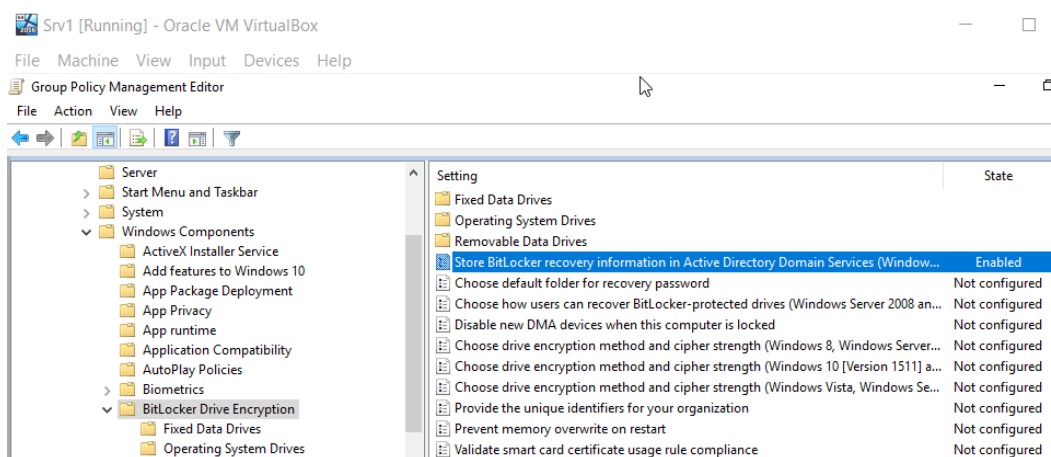


Рисунок 3.31 – Налаштування політики BitLocker

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

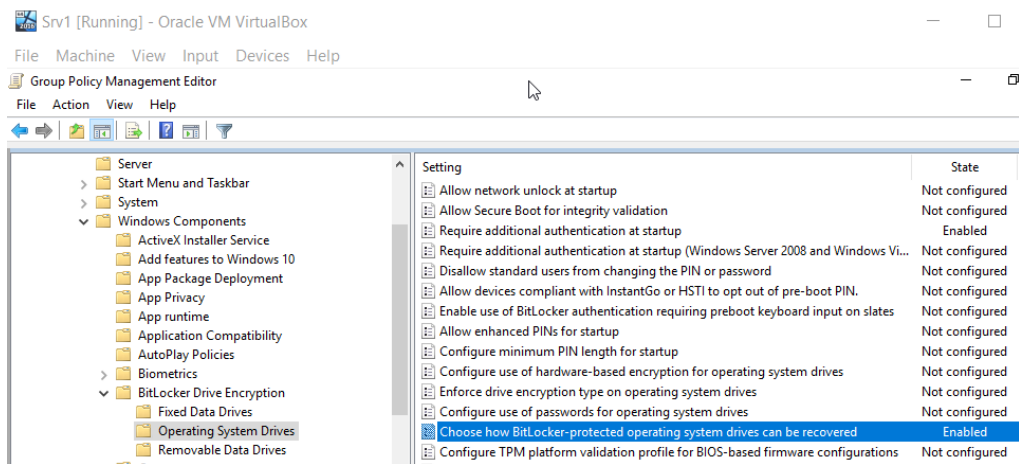


Рисунок 3.32 – Налаштування політики BitLocker

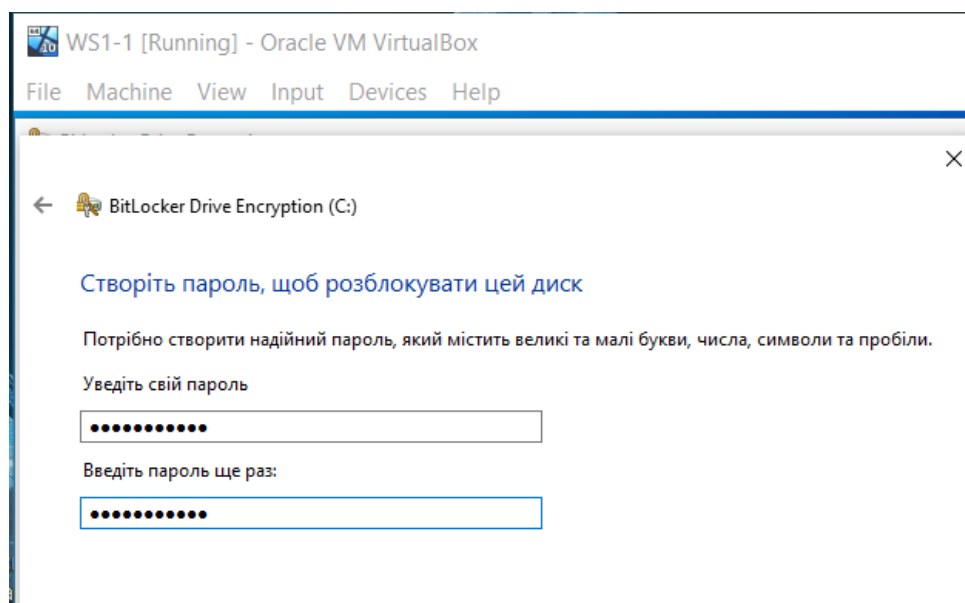


Рисунок 3.33 – Створення паролю для розблокування ПК

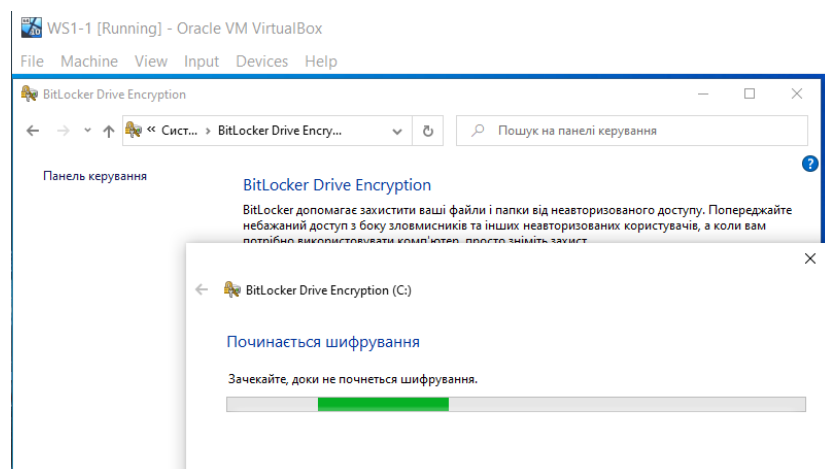


Рисунок 3.34 – Початок шифрування

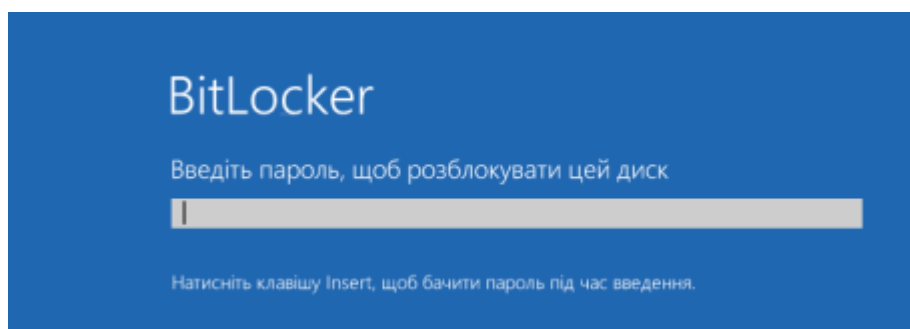


Рисунок 3.35 – Результат увімкнення шифрування жорсткого диску

3.3 Тестування та оцінка ефективності підсистеми

Після налаштування всієї мережі та створення групових політик. Можемо протестувати нашу мережу.

Спершу спробуємо неправильно ввести пароль 3 рази, щоб зрозуміти, чи працює політика паролів (рис. 3.36). Як бачимо, політика працює (рис. 3.37-3.38).

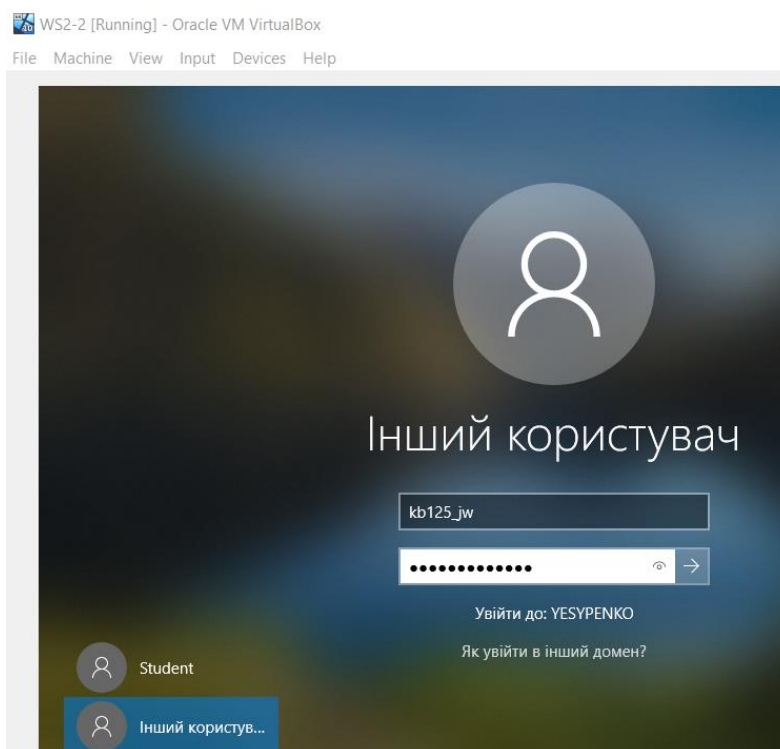


Рисунок 3.36 – Вхід в користувача

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

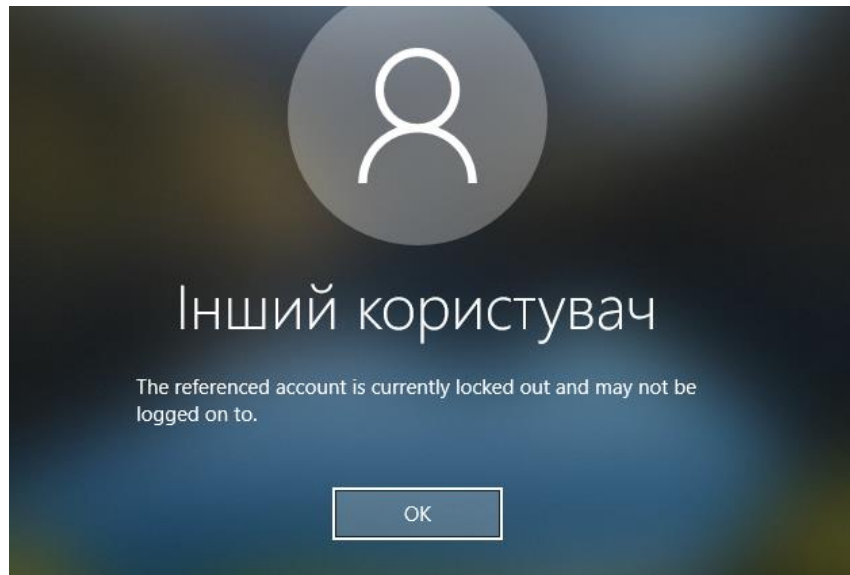


Рисунок 3.37 – Блокування облікового запису після 3 невдалих спроб введення паролю

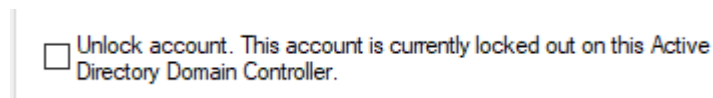


Рисунок 3.38 – Функція для розблокування облікового запису

Далі спробуємо встановити програму, в нашому випадку браузер “Opera”. Дана програма була попередньо завантажена на ПК (рис.3.39).

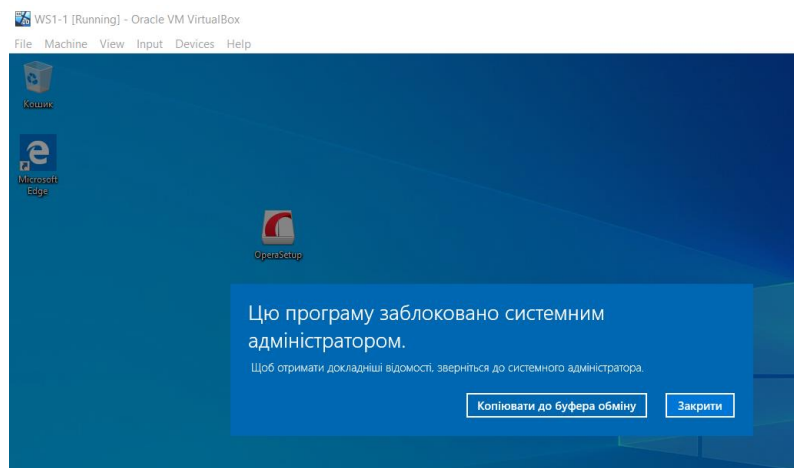


Рисунок 3.39 – Успішна перевірка групової політики, яка забороняє встановлювати програми звичайним користувачам

Тепер протестуємо заборону доступу до командного рядка, яку ми налаштували на рис. 3.24.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

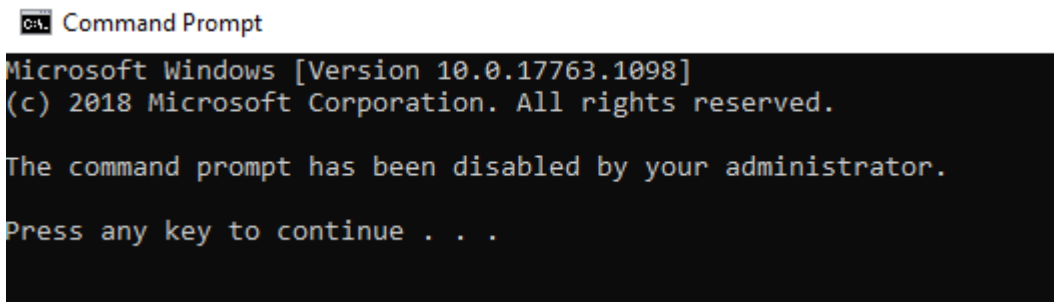


Рисунок 3.40 – Результат перевірки заборони доступу до командного рядку

Також перевіримо чи відобразимуться події у Event Viewer (рис. 3.36).

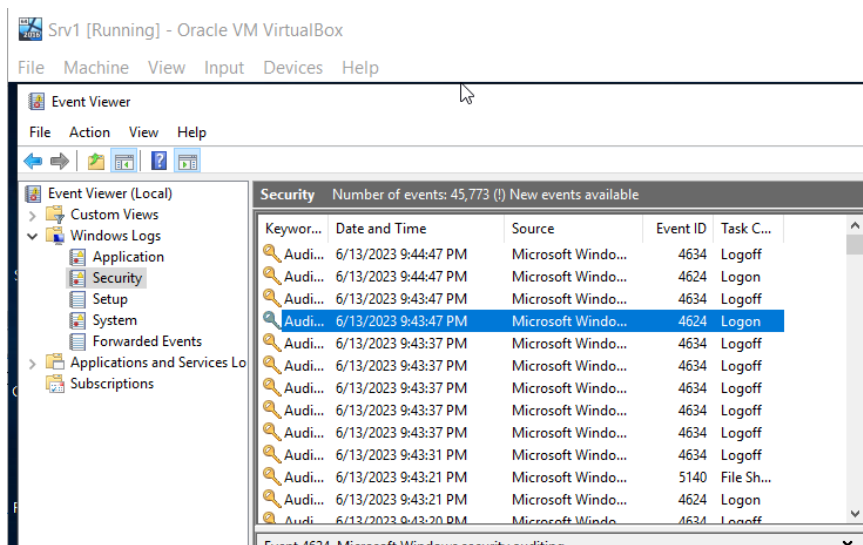


Рисунок 3.41 – Перегляд подій через Event Viewer

Підводячи підсумок тестування, корпоративна мережа працює відповідно до поставлених завдань та має достатній рівень захищеності від інсайдерських атак.

Висновки до третього розділу

У третьому розділі було налагоджено усе обладнання мережі, приготовлено до роботи сервер з Active Directory та налаштовано на ньому групові політики, які необхідні для захисту від інсайдерських ата. Протестовано налаштовані політики безпеки.

ВИСНОВКИ

У даній кваліфікаційній роботі було налаштовано основний захист від інсайдерських атак.

У першому розділі було досліджено причини мотивації порушників та види інсайдерських атак, методи виявлення атак, наприклад: розмежування прав доступу та інші. Також було розглянуто основні вразливості на базі Windows.

У другому розділі було описано та побудовано мережу, яка включає в себе 5 маршрутизаторів, 3 комутатори, 12 робочих станцій та сервер з Active Directory, та проаналізовано можливості вибраних пристроїв. Також була розроблена схема адресації мережі, розглянуто відомості про протоколи OSPF та EIGRP, описано основні характеристики та недоліки цих протоколів, розглянуто модель загроз та розроблено політику безпеки для співробітників.

У третьому розділі було налагоджено обладнання мережі: налаштовано IP-адресацію, VLAN, протоколи OSPF, EIGRP та SSH. Підготовлено до роботи сервер з Active Directory та налаштовано на ньому групові політики, які необхідні для захисту від інсайдерських атак. Після успішного налаштування, мережу було протестовано.

У результаті виконання кваліфікаційної роботи було створено та протестовано проєкт підсистеми захисту від інсайдерських атак Windows-мережі на базі Active Directory.

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

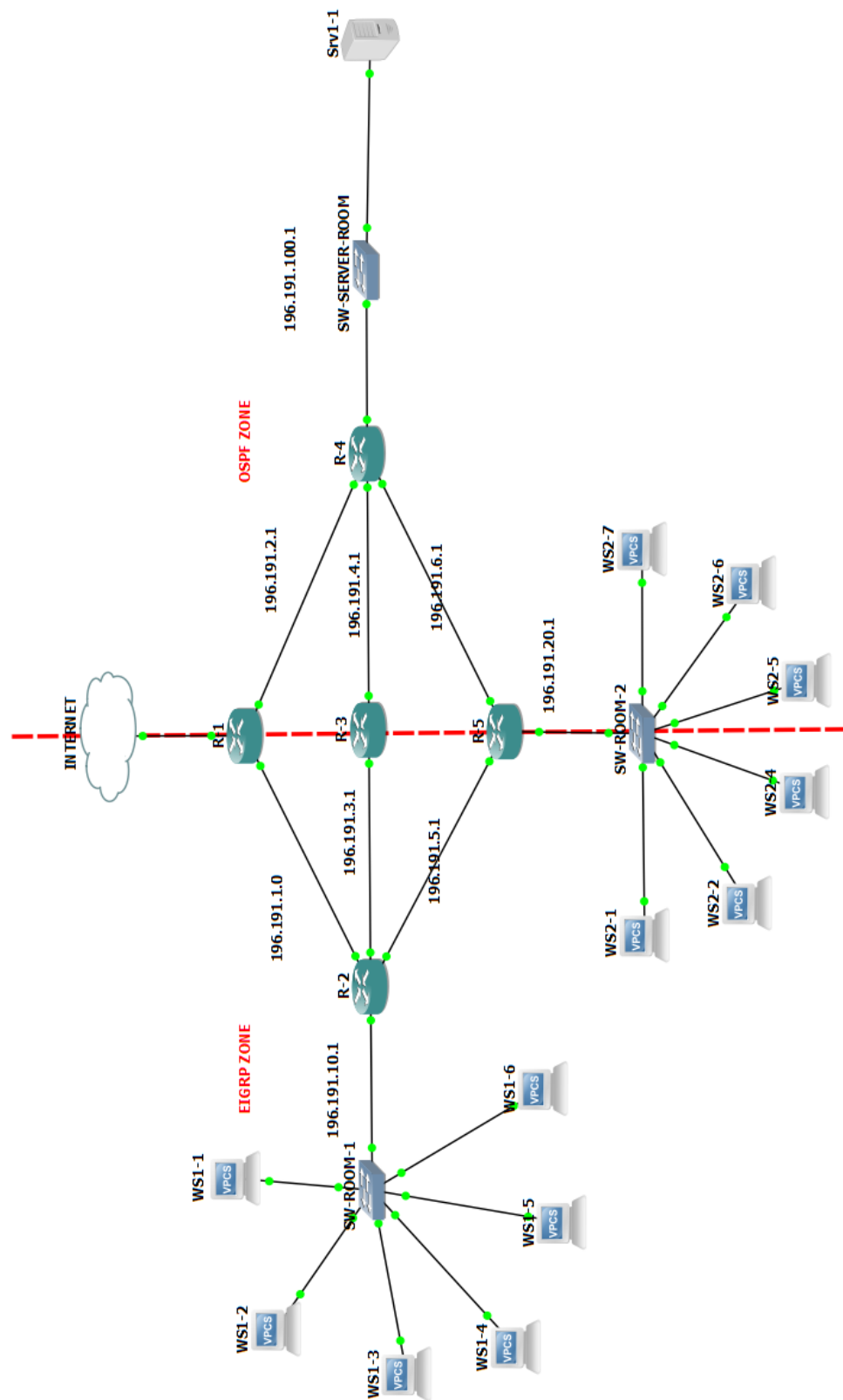
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Best Group Policy settings for effective administration. [Електронний ресурс].
Режим доступу до ресурсу: <https://www.manageengine.com/products/active-directory-audit/kb/best-practices/best-group-policy-settings.html>
2. Cybersecurity Foundations - 5: Threats and Malware. [Електронний ресурс].
Режим доступу до ресурсу: <https://www.rangeforce.com>
3. What are insider threats?. [Електронний ресурс]. Режим доступу до ресурсу:
<https://www.ibm.com/topics/insider-threats>
4. SSH. Що це і для чого?. [Електронний ресурс]. Режим доступу до ресурсу:
<https://hyperhost.ua/info/uk/ssh-shcho-tse-i-dlya-chogo>
5. Cisco 7200 Series Routers. [Електронний ресурс]. Режим доступу до ресурсу:
<https://www.cisco.com/c/en/us/support/routers/7200-series-routers/series.html>
6. Cisco Catalyst 2960. [Електронний ресурс]. Режим доступу до ресурсу:
<https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html>
7. Threat Modeling. [Електронний ресурс]. Режим доступу до ресурсу:
https://owasp.org/www-community/Threat_Modeling
8. Man in the middle (MITM) attack. [Електронний ресурс]. Режим доступу до ресурсу:
<https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
9. How to Prevent DDoS Attack on Router. [Електронний ресурс]. Режим доступу до ресурсу:
<https://ddos-guard.net/en/blog/how-to-prevent-ddos-attack-on-router>
10. Difference between EIGRP and OSPF. [Електронний ресурс]. Режим доступу до ресурсу:
<http://surl.li/imjfi>
11. Group Policy Management in Active Directory. [Електронний ресурс]. Режим доступу до ресурсу:
<https://woshub.com/group-policy-active-directory/>

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				44
Змн.	Арк.	№ докум.	Підпис	Дата		



Додаток Б Лістинг конфігурації пристроїв

```

R-1
Current configuration : 1807 bytes
!
! Last configuration change at 14:50:03
UTC Thu Jun 22 2023
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
!
!
enable secret 5
$1$yQhk$/8WZ89JeMnBUT3jwOKcnz
1
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 5
$1$WhTb$lprH-
gOH7wfH4AAI6bnWtM1
!
redundancy
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
no ip address

```

```

ip nat outside
ip virtual-reassembly in
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
ip nat outside
ip virtual-reassembly in
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 196.191.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 196.191.2.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
!
router eigrp 6
network 192.168.122.0
network 196.191.1.0
redistribute ospf 6 metric 100000 2 255
1 1500
!
router ospf 6
redistribute eigrp 6 subnets
network 196.191.2.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

```

!
ip nat inside source list 1 interface
FastEthernet0/0 overload
!
access-list 1 permit 192.168.122.0
0.0.0.255
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
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
!
End

R-2
Current configuration : 2089 bytes
!
! Last configuration change at 14:52:46
UTC Thu Jun 22 2023
upgrade fpd auto
version 15.2

```

```

service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-2
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$zd7I$yQZ-
ZOd8iZ8xdU.t6rNUKf.
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 5
$1$/HDE$sCya5Mjj1V6zIjG.VZ5N4/
!
redundancy
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 196.191.3.2 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet0/0.10
ip nat inside
ip virtual-reassembly in
!
interface FastEthernet0/1
no ip address

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 196.191.1.2 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 196.191.5.2 255.255.255.252
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Ethernet2/0
no ip address
duplex half
!
interface Ethernet2/0.10
encapsulation dot1Q 10
ip address 196.191.10.1 255.255.255.0
!
interface Ethernet2/1
no ip address
shutdown
duplex half
!
interface Ethernet2/2
no ip address
shutdown
duplex half
!
interface Ethernet2/3
no ip address
shutdown
duplex half
!
!
router eigrp 6
network 196.191.1.0
network 196.191.3.0

```

```

network 196.191.5.0
network 196.191.10.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface
Ethernet2/0.10 overload
!
access-list 1 permit 192.168.122.0
0.0.0.255
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
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
!
End

R-3

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Current configuration : 1879 bytes
!
! Last configuration change at 14:58:08
UTC Thu Jun 22 2023
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-3
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$b1TO$PrH70HX8bz6FKlQMZb2T1
/
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 5
$1$R6dg$hUjdbVYuP6cT3Hg6NZUcG
0
!
redundancy
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 196.191.3.1 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto

```

```

speed auto
!
interface FastEthernet0/1
ip address 196.191.4.1 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
!
router eigrp 6
network 196.191.3.0
redistribute ospf 6 metric 100000 2 255
1 1500
!
router ospf 6
redistribute eigrp 6 subnets
network 196.191.4.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
access-list 1 permit 192.168.122.0
0.0.0.255
access-list 1 permit 196.191.3.0 0.0.0.3
access-list 1 permit 196.191.4.0 0.0.0.3
access-list 1 permit 196.191.10.0
0.0.0.255
access-list 1 permit 196.191.100.0
0.0.0.255

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

access-list 1 permit 196.191.20.0
0.0.0.255
access-list 1 deny any
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
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
!
End

```

```

R-4
Current configuration : 2446 bytes
!
! Last configuration change at 15:01:19
UTC Thu Jun 22 2023
upgrade fpd auto
version 15.2

```

```

service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-4
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$cN5B$pQ98XzYFL06fqLE7u7WPc
0
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
username admin privilege 15 secret 5
$1$a0V0$hKf771Vgt/6hQ0qKCudBE.
!
redundancy
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
no ip address
ip nat outside
ip virtual-reassembly in
shutdown
duplex auto
speed auto

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet0/1
 ip address 196.191.4.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet1/0
 ip address 196.191.6.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 196.191.2.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Ethernet2/0
 no ip address
 ip nat inside
 ip virtual-reassembly in
 duplex half
!
interface Ethernet2/0.100
 encapsulation dot1Q 100
 ip address 196.191.100.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Ethernet2/1
 no ip address
 shutdown
 duplex half
!
interface Ethernet2/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet2/3
 no ip address
 shutdown

```

```

duplex half
!
router ospf 6
 network 196.191.2.0 0.0.0.3 area 0
 network 196.191.4.0 0.0.0.3 area 0
 network 196.191.6.0 0.0.0.3 area 0
 network 196.191.100.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface
Ethernet2/0.20 overload
!
access-list 1 permit 192.168.122.0
0.0.0.255
access-list 1 permit 196.191.2.0 0.0.0.3
access-list 1 permit 196.191.4.0 0.0.0.3
access-list 1 permit 196.191.6.0 0.0.0.3
access-list 1 permit 196.191.10.0
0.0.0.255
access-list 1 permit 196.191.100.0
0.0.0.255
access-list 1 permit 196.191.20.0
0.0.0.255
access-list 1 deny any
no cdp log mismatch duplex
!
!
control-plane
!
!
mgcp profile default
!
!
!
gatekeeper
shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
End

```

```

R-5
Current configuration : 2378 bytes
!
! Last configuration change at 15:03:03
UTC Thu Jun 22 2023
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R-5
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$vOgr$C17FmNgW0kVnE9qssyIy1
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!

```

```

username admin privilege 15 secret 5
$1$5GVg$pphv1g/VmHO5eL7Dyma4b
1
!
redundancy
!
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 196.191.6.1 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 196.191.5.1 255.255.255.252
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Ethernet2/0
no ip address
ip nat inside
ip virtual-reassembly in
duplex half
!
interface Ethernet2/0.20
encapsulation dot1Q 20
ip address 196.191.20.1 255.255.255.0
ip nat inside

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip virtual-reassembly in
!
interface Ethernet2/1
no ip address
shutdown
duplex half
!
interface Ethernet2/2
no ip address
shutdown
duplex half
!
interface Ethernet2/3
no ip address
shutdown
duplex half
!
!
router eigrp 6
network 196.191.5.0
network 196.191.20.0
redistribute ospf 6 metric 100000 2 255
1 1500
!
router ospf 6
redistribute eigrp 6 subnets
network 196.191.6.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface
Ethernet2/0.100 overload
!
access-list 1 permit 192.168.122.0
0.0.0.255
access-list 1 permit 196.191.5.0
0.0.0.255

```

```

access-list 1 permit 196.191.6.0
0.0.0.255
access-list 1 permit 196.191.10.0
0.0.0.255
access-list 1 permit 196.191.100.0
0.0.0.255
access-list 1 permit 196.191.20.0
0.0.0.255
access-list 1 deny any
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
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
!
end

```

		Єсипенко В. І.			КІК.КР.Б – 125 – 5 – ПЗ	Арк.
		Головня О. С.				11
Змн.	Арк.	№ докум.	Підпис	Дата		