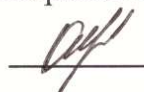


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми забезпечення безпеки
корпоративної мережі на базі Active Directory»

Виконала: студентка 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»

 Ольга ШЕРЕНГІВСЬКА

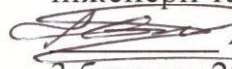
Керівник: старший викладач кафедри КІ та КБ

 Вадим МИКОЛАЙЧУК

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

 Олена ГОЛОВНЯ

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студентка: Шеренгівська Ольга Анатоліївна

Тема роботи: «Проект підсистеми забезпечення безпеки корпоративної мережі на базі Active Directory»

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

Термін здачі студентом закінченої роботи 10 червня 2025 р.

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

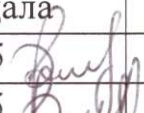
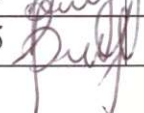
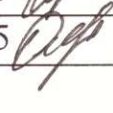
Методи та засоби підвищення безпеки Active Directory

Корпоративна мережа організації

Обладнання й програмне забезпечення:

1. Windows Server 2019 Standard
2. Windows 10 Education
3. Active Directory
4. Cisco 3725
5. Cisco Catalyst 3560
6. Cisco WS-C2960-24NN-L

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

Розділ	Консультант	Підпис, дата	
		Завдання видала	Завдання прийняла
1	Трокоз Є.М	31.03.2025 	31.03.2025 
2-3	Трокоз Є.М	27.05.2025 	27.05.2025 

Студентка



Ольга ШЕРЕНГІВСЬКА

Керівник



Вадим МИКОЛАЙЧУК

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2025	Виконано
2	Аналіз літературних джерел та нормативної документації	06.03.2025 – 28.03.2025	Виконано
3	Формування мети, завдань, об'єкта та предмета дослідження	12.04.2024	Виконано
4	Розробка технічного завдання на проектування підсистеми захисту	21.04.2025 – 12.05.2025	Виконано
5	Проектування топології мережі	17.05.2025	Виконано
6	Реалізація мережевої інфраструктури та налаштування AD	20.05.2025	Виконано
7	Налаштування засобів захисту. GPO, аудит, контроль доступу	27.05.2025	Виконано
8	Тестування, перевірка ефективності впроваджених рішень	01.06.2025	Виконано
9	Оформлення пояснювальної записки	10.06.2025	Виконано
10	Оформлення презентації	23.06.2025	Виконано
11	Захист	26.06.2025	Виконано

Студентка



Ольга ШЕРЕНГІВСЬКА

Керівник



Вадим МИКОЛАЙЧУК

АНОТАЦІЯ

Пояснювальна записка до кваліфікаційної роботи складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатку.

Обсяг записки становить 87 сторінок, вона містить 61 рисунок і 9 таблиць. Список використаних джерел охоплює 15 найменувань та розміщений на 2 сторінках. Метою випускної кваліфікаційної роботи є розробка та впровадження підсистеми безпеки корпоративної мережі, що базується на Active Directory, із урахуванням сучасних вимог до інформаційної безпеки, політик доступу, контролю подій та автоматизації адміністративних задач.

У ході роботи визначено основні загрози та вразливості, притаманні службі каталогів Active Directory, розглянуто особливості її впровадження у корпоративному середовищі, проаналізовано сучасні методи захисту, включаючи принцип найменших привілеїв, сегментацію мережі на основі VLAN, резервування шлюзів за допомогою HSRP та аудит безпеки. Показано розробку топології корпоративної мережі у середовищі GNS3, а також реалізацію засобів контролю доступу та обмеження повноважень адміністративних облікових записів. В роботі впроваджено групові політики безпеки (GPO), обмеження на запуск скриптів, використання USB-пристроїв для зберігання даних, заборону PowerShell, налаштування PAW-станцій.

Наведено результати тестування системи захисту: підтверджено ефективність впроваджених політик, перевірено контроль доступу до ресурсів, дотримання обмежень щодо облікових записів і журналювання подій. Запропоновано PowerShell-скрипти для автоматичного збору інформації про неактивних користувачів, політики безпеки та події залогуювання.

Ключові слова: ACTIVE DIRECTORY, КОРПОРАТИВНА МЕРЕЖА, GPO, АУДИТ, КОНТРОЛЬ ДОСТУПУ, WINDOWS SERVER, VLAN, POWERSHELL.

					ККІК.КР.Б – 125 – 19 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Шеренгівська О.А.		26.06.25	Проектування та реалізація підсистеми захисту корпоративної мережі на базі Active Directory	Літ.	Арк.
Керівник		Миколайчук В.В.		26.06.25			4
Реценз.		Головня О.С.		26.06.25		Аркушів	87
Н. контр.		Миколайчук В.В.		26.06.25		ФІКТ Гр. КБ-21-2	
Завтверд.		Єфіменко А.А.		26.06.25			

ANNOTATION

The explanatory note to the qualification thesis consists of a list of abbreviations, an introduction, three chapters, conclusions, a list of references, and an appendix.

The total volume of the explanatory note is 87 pages and includes 61 figures and 9 tables. The list of references comprises 15 sources and is presented on 2 pages.

The aim of this qualification thesis is the development and implementation of a corporate network security subsystem based on Active Directory, taking into account modern requirements for information security, access control policies, event monitoring, and automation of administrative tasks.

The work identifies the main threats and vulnerabilities inherent in the Active Directory directory service, considers the specifics of its implementation in a corporate environment, and analyzes modern protection methods, including the principle of least privilege, VLAN-based network segmentation, gateway redundancy using HSRP, and security auditing.

The project presents the development of a corporate network topology in the GNS3 environment, as well as the implementation of access control tools and restrictions on administrative account privileges.

Group Policy Objects (GPOs) were implemented, along with restrictions on script execution, the use of USB storage devices, PowerShell access, and the configuration of PAW (Privileged Access Workstations).

The results of the security system testing are provided: the effectiveness of the implemented policies was confirmed, access control to resources was verified, compliance with account restrictions was ensured, and event logging was tested. PowerShell scripts were proposed for the automated collection of information about inactive users, security policies, and logon events.

Keywords: ACTIVE DIRECTORY, CORPORATE NETWORK, GPO, AUDIT, ACCESS CONTROL, WINDOWS SERVER, VLAN, POWERSHELL.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ОСОБЛИВОСТІ ТА ЗАГРОЗИ ДЛЯ СИСТЕМИ ACTIVE DIRECTORY У КОРПОРАТИВНИХ МЕРЕЖАХ	10
1.1 Роль служби Active Directory у корпоративних мережах.....	10
1.2 Вразливості та загрози Active Directory.	11
1.3 Основні принципи побудови захисту Active Directory.....	12
Висновки до першого розділу.....	14
РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖІ НА БАЗІ ACTIVE DIRECTORY	16
2.1 Вибір програмного та апаратного забезпечення для проєктування мережі.....	16
2.1.1 Вибір маршрутизатора для мережі	17
2.1.2 Вибір комутаторів для мережі	18
2.1.3 Версія Windows у реалізації підсистеми захисту.....	19
2.2 Вибір методів та інструментів захисту	21
2.3 Впровадження політик безпеки для захисту AD:	21
2.3.1 Парольна політика.....	21
2.3.2 Політика блокування облікових записів	22
2.3.3 Аудит безпеки.....	23
2.3.4 Обмеження адміністративного доступу.....	24
2.3.5 Інші політики безпеки в Active Directory.....	24
2.4 Налаштування корпоративної мережі	25
Висновки до другого розділу.....	33
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ ACTIVE DIRECTORY.....	35
3.1 Встановлення служби каталогів Active Directory та його налаштування у Windows Server 2019.....	35
3.2 Розробка та впровадження захисту мережі Active Directory	38
3.3 Перевірка роботи виконаних налаштувань.	49

Висновок до третього розділу.....	58
ВИСНОВКИ.....	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	61
ДОДАТКИ.....	63
ДОДАТОК А.....	64
ДОДАТОК Б	65
ДОДАТОК В.....	79

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

GPO – Group Policy Object

OU – Organizational Unit

VLAN – Virtual Local Area Network

STP – Spanning Tree Protocol

RSTP – Rapid Spanning Tree Protocol

SSH – Secure Shell

PAW – Privileged Access Workstation

ОС – Операційна система

ПЗ – Програмне забезпечення

HSRP – Standby Router Protocol

GNS3 – Graphical Network Simulator-3

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. Сучасні інформаційні системи відіграють ключову роль у забезпеченні функціонування бізнесу, державного управління та інших сфер діяльності. Зі зростанням ролі ІТ зростає й кількість кіберзагроз, що ставлять під ризик безперервність роботи, конфіденційність даних та доступ до ресурсів. У середовищах Windows критично важливим компонентом є служба каталогів Active Directory, яка забезпечує централізоване управління користувачами, правами доступу та політиками безпеки. Вразливість AD через неналежний захист може призвести до масштабних атак і витоку даних.

Метою кваліфікаційної роботи є розробка та впровадження підсистеми безпеки корпоративної мережі на основі Active Directory, що включає налаштування групових політик, автоматизований аудит подій, контроль доступу та оцінку ефективності реалізованих рішень у тестовому середовищі.

Визначена мета обумовлює наступні завдання:

- проаналізувати особливості та вразливості служби AD;
- дослідити загрози безпеці та принципи захисту AD;
- реалізувати механізми захисту;
- провести тестування.

Об’єктом дослідження є корпоративна мережа організації, побудована з використанням Windows Server і служби Active Directory.

Предмет дослідження – методи та засоби підвищення безпеки Active Directory у корпоративному середовищі.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту мережі, що забезпечує централізоване управління доступом, моніторинг подій, обмеження привілеїв та автоматизацію щоденних адміністративних дій із використанням GPO і PowerShell у тестовому середовищі.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ОСОБЛИВОСТІ ТА ЗАГРОЗИ ДЛЯ СИСТЕМИ ACTIVE DIRECTORY У КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Роль служби Active Directory у корпоративних мережах.

Служба каталогів Active Directory (AD) є базовим інструментом для централізованого управління корпоративними мережами, які функціонують на базі Windows. Вона дозволяє організувати структуру мережі у вигляді доменів, організаційних одиниць (OU), користувачів, комп'ютерів та політик безпеки. Така ієрархічна модель сприяє централізованому керуванню обліковими записами, політиками доступу, автентифікацією та іншими аспектами адміністрування. На рисунку 1.1 наведено ієрархію AD.

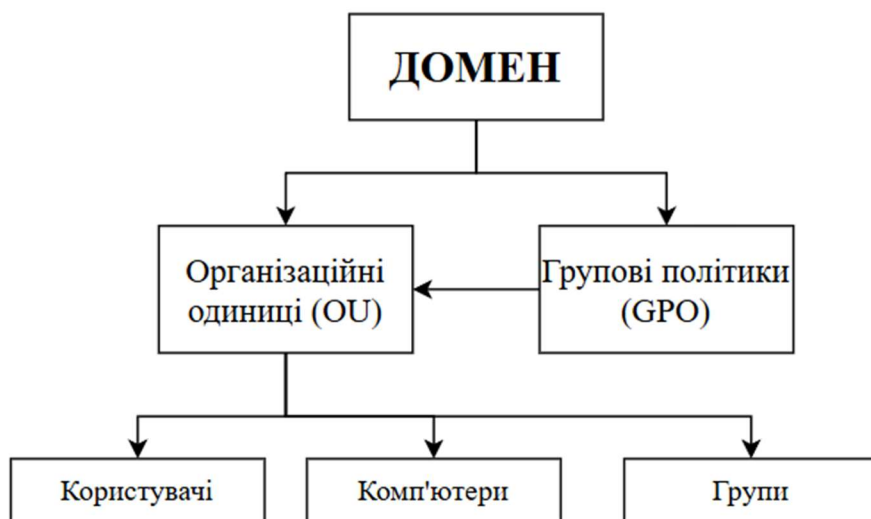


Рисунок 1.1 – Візуалізація структури AD

Active Directory (AD) є централізованою системою каталогів, що використовується для управління мережами на основі Windows. Завдяки своїй ієрархічній і розподіленій архітектурі AD дозволяє організаціям ефективно масштабувати ресурси та адмініструвати мільйони об'єктів, таких як користувачі, комп'ютери, групи, спільні файли та мережеві пристрої. На практиці це означає, що адміністратор не витрачає години на налаштування кожної конкретної машини, а управління кожною машиною відбувається з контролера домену [1].

Однак, якими б не були переваги Active Directory, але централізація даних і широке впровадження AD роблять її привабливою мішенню для кібератак.

Дана служба має безліч груп, які забезпечують різні ролі та рівні авторизації і тому ними необхідно ретельно керувати та захищати в усіх організаціях, щоб зменшити ризик несанкціонованого доступу зловмисників через потенційні помилки в налаштуваннях.

1.2 Вразливості та загрози Active Directory.

Active Directory розроблена як надійна платформа, але це не означає, що вона автоматично захищена від усіх можливих загроз. Основні загрози для Active Directory, пов'язані з некоректною конфігурацією, слабкими паролями та відсутністю належного журналювання, можуть стати причиною серйозних атак на мережу. AD як і будь-які інші елементи мережі потребує уваги, контролю та регулярного обслуговування. Часто помилки виникають через неналежне налаштування або через нехтування базовими правилами безпеки.

Однак є й інші, більш специфічні загрози, які можуть значно вплинути на безпеку організації, якщо не вжити належних заходів.

У таблиці 1.1 було наведено список загроз, які можуть виникнути в середовищі Active Directory, та практичні заходи щодо їх зниження:

Таблиця 1.1

Потенційні загрози

Тип загрози	Як це виглядає на практиці	Що можна зробити, щоб захиститись
Атаки грубої сили	Зловмисник запускає автоматичну програму, яка перебирає тисячі паролів, поки не вгадає правильний. Якщо пароль був простий, то злам відбудеться максимально швидко.	Складна політика паролів, а також регулярне оновлення нових паролів.
Латеральне переміщення	Зловмисник після отримання доступу до одного пристрою переміщується мережею, зламує інші станції або облікові записи, щоб поширити вплив.	Сегментація мережі, обмеження доступу, виявлення підозрілої активності, мінімізація сесій адміністраторів
Підвищення привілеїв	Зловмисник, маючи базові права, намагається отримати доступ до прав адміністратора через експлойти, неправильні налаштування або службові облікові записи.	Принцип найменших привілеїв, контроль привілеїв, регулярний аудит прав, захист чутливих груп (Domain Admins).

Атаки на Kerberos	Зловмисник перехоплює дані, які Kerberos передає для автентифікації і намагається використати ті дані повторно, ніби маскується під справжнього користувача.	Регулярне оновлення системи, відстеження аномальних подій в журналах.
-------------------	--	---

Отже, можна сказати, що загрози для Active Directory є численними і постійно еволюціонують, тому список загроз наведених в таблиці 1.1 не є вичерпним. Однак, розуміння цих основних загроз і впровадження правильної безпекової політики допоможуть значно знизити ймовірність успішних атак. Зокрема, своєчасна і ефективна реалізація заходів безпеки дозволить захистити критично важливі цифрові активи і зберегти цілісність мережі [2].

1.3 Основні принципи побудови захисту Active Directory

Забезпечення надійного функціонування служби каталогів Active Directory (AD) є одним із найважливіших елементів стратегії кіберзахисту корпоративного середовища. Сама по собі наявність AD не гарантує безпеки. Щоб мінімізувати ризики та знизити вразливість, потрібно дотримуватись низки концептуальних і практичних принципів, які охоплюють як технічні, так і організаційні аспекти.

Одним із найфундаментальніших підходів, що набув широкого визнання у міжнародній практиці, є принцип найменших привілеїв. Його суть полягає в обмеженні доступу користувачів, служб і адміністраторів лише тими правами, які є необхідними для виконання їхніх функціональних обов'язків. Такий підхід дозволяє мінімізувати потенційну шкоду у випадку, якщо облікові дані буде скомпрометовано, і запобігає ескалації привілеїв, яка є поширеною технікою атак.

Однак сам по собі розподіл прав не є достатнім без належного впорядкування адміністративного доступу. У сучасних організаціях дедалі частіше застосовується концепція ієрархічного (tiered) адміністрування, коли повноваження чітко поділено між різними рівнями інфраструктури – від критично важливих контролерів домену до звичайних робочих станцій. Така модель дає змогу уникнути змішування ролей і виключити ситуації, коли

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

адміністративний обліковий запис із надмірними правами використовується для рутинної діяльності.

Особливу увагу слід приділяти безпеці адміністративних станцій. Згідно з рекомендаціями Microsoft, «не допускається адміністрування довіреної системи з менш захищеного хоста. Адміністративні станції не повинні містити стороннє програмне забезпечення, таке як поштові клієнти, браузер чи офісні застосунки» [3].

Не менш важливою є практика своєчасного оновлення програмного забезпечення. Уразливості, виявлені в операційних системах і службах AD, часто стають об'єктами активної експлуатації. Несвоєчасне застосування оновлень може призвести до того, що навіть добре налаштована система стане вразливою до вже відомих загроз. Тому розробка політики управління оновленнями, яка охоплює як сервери, так і клієнтські пристрої, є обов'язковою умовою для підтримки безпечного стану AD.

Поряд із профілактичними заходами важливу роль відіграє моніторинг. Постійний контроль за подіями у домені дозволяє виявляти ознаки компрометації на ранньому етапі. Це можуть бути як аномальні спроби входу, так і підозрілі зміни конфігурацій чи політик безпеки. Впровадження централізованих систем журналювання, а також налаштування сповіщень про критичні події значно підвищують оперативність реагування та дозволяють вчасно локалізувати інцидент.

Також уваги потребують контролери домену, які є центральними вузлами Active Directory. Їхній захист має бути багаторівневим: від фізичного ізолювання до налаштування, обмеження вхідних підключень і використання лише спеціалізованих адміністративних станцій. Крім того, критично важливою є заборона виходу на зовнішні ресурси.

Варто зазначити, що навіть найсучасніша технологічна інфраструктура залишається вразливою до атак до поки в ній є люди, оскільки люди вразливі до атак соціальної інженерії, тим паче якщо вони недостатньо обізнані у питаннях інформаційної безпеки. Саме тому безперервне навчання персоналу має стати

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

частиною загальної стратегії захисту. Це стосується не лише адміністраторів, а й усіх користувачів, які взаємодіють з доменом. Тренінги, симуляції фішингових атак, короткі інструкції – усе це дозволяє формувати культуру безпеки та запобігати інцидентам, які починаються з людської помилки.

І, нарешті, жодна система не є ідеальною без постійного тестування. Аудит безпеки, сканування на вразливості, аналіз конфігурацій та періодичне моделювання інцидентів дозволяють не лише виявляти слабкі місця, а й оцінювати ефективність наявних заходів. Такий підхід забезпечує адаптивність захисту до нових викликів і гарантує відповідність вимогам як внутрішніх стандартів компанії, так і зовнішніх регуляторів, наприклад ISO/IEC 27001 або NIST SP 800-53.

У сукупності описані принципи утворюють основу стратегічного підходу до захисту служби каталогів. Вони не є взаємовиключними – навпаки, лише одночасне і комплексне їхнє застосування дозволяє побудувати справді стійку до загроз інфраструктуру, яка ефективно функціонує навіть у складних умовах сучасного кіберпростору. Ще одним не менш важливим елементом є тестування. Регулярний аудит, перевірка безпеки, сканування на вразливості та моделювання атак дозволяють виявити слабкі місця до того, як ними скористаються.

Висновки до першого розділу

У першому розділі було досліджено роль служби Active Directory у корпоративних мережах, її архітектуру, призначення та функціональні можливості. Акцент зроблено на тому, що AD є основою централізованого управління доступом, обліковими записами, політиками безпеки та ресурсами. Виявлено, що саме через свою критичну роль у середовищі Windows, AD є однією з найбільш привабливих цілей для злоумисників.

Здійснено аналіз типових загроз, серед яких ключовими є атаки грубої сили, латеральне переміщення в мережі, підвищення привілеїв та зловживання протоколом Kerberos. Встановлено, що значна частина вразливостей пов'язана не зі самою технологією AD, а з людським фактором: недбалістю у

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштуванні, нехтуванням базовими політиками безпеки та відсутністю моніторингу. Було розглянуто приклади того, як зловмисник, отримавши доступ до одного облікового запису, може поступово захопити повний контроль над мережею, якщо в системі не реалізовано принцип найменших привілеїв.

На основі аналізу сформульовано перелік ключових принципів побудови безпеки AD: обмеження прав доступу, моніторинг та аудит подій, ізоляція контролерів домену та підвищення обізнаності персоналу. Встановлено, що без належної реалізації цих принципів навіть добре побудована інфраструктура може бути вразливою до типових атак.

Таким чином, у цьому розділі не лише охарактеризовано базові компоненти AD, але й сформовано практичну основу для наступних етапів проєкту — зокрема, проєктування топології, реалізації політик безпеки, контролю доступу та побудови надійного середовища корпоративної мережі. Отримані висновки лягли в основу подальшої розробки підсистеми захисту та її реалізації в тестовому середовищі.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖІ НА БАЗІ ACTIVE DIRECTORY

2.1 Вибір програмного та апаратного забезпечення для проєктування мережі

Для реалізації проєкту використано програмне середовище GNS3, яке дозволяє створювати та тестувати топологію мережі без потреб у фізичному обладнанні. GNS3 (Graphical Network Simulator-3) є одним із найпоширеніших інструментів для моделювання комп'ютерних мереж, який дозволяє створювати віртуальні топології з використанням реального мережевого обладнання або емуляційних образів. Завдяки підтримці широкого спектра пристроїв і протоколів, GNS3 став незамінним середовищем для тестування, навчання та розробки мережевих рішень, зокрема в рамках проєктування системи захисту корпоративної мережі[4].

Однією з ключових переваг GNS3 є можливість інтеграції з реальними операційними системами. Це дозволяє запускати віртуальні машини на базі Windows Server, Linux або клієнтських ОС, таких як Windows 10, безпосередньо у змодельованій топології. Таким чином, інженер або дослідник отримує змогу проводити комплексне тестування взаємодії між мережевими пристроями, серверними ролями, клієнтськими станціями та політиками безпеки в умовах, наближених до реальних.

Значною перевагою є і підтримка роботи з образами Cisco IOS, що забезпечує точне відтворення функціоналу маршрутизаторів і комутаторів Cisco. Це дозволяє реалізовувати такі механізми, як VLAN, HSRP, SSH, NAT, DHCP та інші функції рівнів OSI, необхідні для створення складних мережевих структур. У контексті дипломної роботи середовище GNS3 було використано для моделювання кількох VLAN-сегментів, налаштування резервування шлюзів, реалізації інтервіланової маршрутизації та перевірки доступності домен-контролера з різних сегментів мережі.

Крім технічних функцій, GNS3 також забезпечує візуалізацію мережевої інфраструктури. Графічний інтерфейс дає змогу інтуїтивно розташовувати

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

пристрої, створювати логічні з'єднання, маркувати сегменти мережі та спостерігати за активністю інтерфейсів. Це значно полегшує процес проєктування та подальшого аналізу побудованої інфраструктури, особливо у випадках, коли потрібно продемонструвати функціонування мережі стороннім особам — керівництву, викладачам, аудиторам або замовникам.

Важливим є також те, що GNS3 підтримує імпорт власних шаблонів та сценаріїв, що дозволяє створити базову модель для багаторазового використання або змодельовати специфічні ситуації, пов'язані з інцидентами, перевіркою на проникнення або реакцією на збої.

Таким чином, використання GNS3 у межах кваліфікаційної роботи дозволило реалізувати повноцінну модель корпоративної мережі з підтримкою доменної інфраструктури, засобів контролю доступу та перевірки резервування. Це середовище не лише сприяло глибшому розумінню архітектури мережі, але й забезпечило наочність, точність тестування та гнучкість у налаштуванні без ризику для реальних систем.

2.1.1 Вибір маршрутизатора для мережі

У межах проєктування корпоративної мережі ключову роль відіграє маршрутизатор, який забезпечує маршрутизацію між VLAN, доступ до зовнішніх ресурсів, фільтрацію трафіку, а також впровадження політик безпеки.

Для цілей емуляції у середовищі GNS3 використано модель Cisco 3725, яка є логічним еквівалентом базового маршрутизатора з підтримкою багатьох протоколів. Даний маршрутизатор зумовлений сумісністю з емулятором, простотою налаштування та підтримкою необхідних функцій для моделювання мережевої логіки.

Однак, для реального впровадження рекомендовано використовувати сучасніші рішення, наприклад, маршрутизатори серії Cisco ISR 4321 або 4331 які мають розширену підтримку VPN, шифрування трафіку апаратними засобами, віртуалізацію сервісів, інтеграції з системами автентифікації [5].

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатори серії ISR 4000 оптимізовані для середовищ з високими вимогами до доступності та безпеки. Інформація щодо можливостей доступна на офіційному сайті Cisco.



Рисунок 2.1 – Маршрутизатор Cisco 3725

У таблиці 2.1 було наведено порівняння описаних маршрутизаторів.

Таблиця 2.1

Характеристики маршрутизаторів Cisco

Характеристика	Cisco 3725 (використовується в проєкті)	Cisco 4321 ISR	Cisco 4331 ISR
Призначення	Навчальна модель корпоративної мережі в GNS3	Реальна мережа малого офісу	Реальна мережа середнього бізнесу
Переваги	Сумісність з GNS3, підтримка VLAN, HSRP, ACL, NAT	Висока інтеграція, енергоефективність, VPN	Потужність, SD-WAN, масштабованість
Пропускна здатність	10–30 Mbps (достатньо для симуляцій)	До 100 Mbps	До 300 Mbps
Інтерфейси	2x FastEthernet, модулі WIC/NM	2x GE, 1x NIM	3x GE, 2x NIM
Операційна система	Cisco IOS 12.x (adventerprisek9)	Cisco IOS XE	Cisco IOS XE
Підтримка HSRP	+	+	+
GNS3-сумісність	Емулюється безпосередньо	Обмежена через IOU/VIRL	Обмежена через IOU/VIRL
Підтримка VLAN, ACL, NAT	+	+	+
Оптичні інтерфейси (SFP)	-	+	+
Типова роль у проєкті	Основний і резервний маршрутизатор у дипломній мережі	Фізичний маршрутизатор філії	Центр мережі підприємства

2.1.2 Вибір комутаторів для мережі

У побудові корпоративної мережі комутатори поєднують пристрої в межах VLAN, розподіляють трафік і забезпечують стабільність роботи всієї

інфраструктури. У даній мережі використано два рівні комутаційного обладнання:

Комутатори управління – Cisco Catalyst 3560.

Згідно з офіційною технічною документацією Cisco Systems, комутатор серії Catalyst 3560 потужний та надійний пристрій, через який проходить увесь критичний трафік між серверами, маршрутизаторами та іншими вузлами. Він дає змогу реалізувати агрегацію каналів, моніторинг і безпеку трафіку [6].



Рисунок – 2.2 Комутатор Cisco Catalyst 3560

Комутатори доступу – Cisco WS-C2960-24TT-L

Простіші, але цілком ефективні комутатори. Вони з'єднують робочі станції в офісах і надають базову функціональність. Дана модель виконує основні мережеві функції: VLAN, з'єднання trunk та базові механізми безпеки [7].

Поділ на рівні комутації дозволяє підтримувати чітку структуру мережі, підвищити її надійність та забезпечити можливість масштабування у майбутньому.



Рисунок – 2.3 Комутатор Cisco WS-C2960-24NN-L

2.1.3 Версія Windows у реалізації підсистеми захисту

У процесі побудови імітаційної корпоративної мережі з провадженням служби Active Directory було використано операційну систему Windows 10

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Education. Вибір цієї версії зумовлений доступністю відповідної освітньої ліцензії у межах навчального закладу.

Варто зазначити, що відповідно до офіційної документації Microsoft, Windows 10 Education базується на редакції Enterprise і містить аналогічні функціональні можливості щодо корпоративного управління та забезпечення безпеки [8]. Це включає:

- підтримку приєднання до домену (Domain Join);
- роботу з груповими політиками (GPO);
- підтримку BitLocker, AppLocker, Device Guard та інших механізмів безпеки.

Усі функції, які необхідні для налаштування домену, впровадження політик безпеки та контролю доступу, повністю доступні у використанні даної нам ОС. Це дозволяє реалізувати підсистему захисту Active Directory без обмежень.

Варто зазначити, що для серверної частини інфраструктури використовувалась операційна система Windows Server 2019 Standard. Попри наявність новішої версії Windows Server 2022 та оголошеної Windows Server 2025, вибір версії 2019 зумовлений апаратними обмеженнями середовища віртуалізації та високими системними вимогами новіших ОС [9].

В межах дипломного проєкту редакція Standard виявилася оптимальним вибором. На відміну від редакції Datacenter, яка орієнтована на масштабні дата-центри та вимагає значно вищих фінансових і технічних ресурсів, версія Standard має всі необхідні функції для розгортання домену, але без надлишкових сервісів, таких як підтримка необмеженої кількості віртуальних машин, Shielded VMs чи кластерних сховищ.

Таким чином, поєднання Windows 10 Education на клієнтських машинах та Windows Server 2019 Standard на серверній стороні дозволило реалізувати підсистему захисту корпоративної мережі з урахуванням сучасних вимог до інформаційної безпеки та технічних обмежень навчального середовища.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Вибір методів та інструментів захисту

Щоб керувати безпекою в корпоративній мережі було не хаотичним, а чітко структурованим, ми використовуємо групові політики – GPO. Це основний інструмент, що дозволяє централізовано налаштовувати правила, які автоматично застосовуються до користувачів та кінцевих пристроїв у домені. Наприклад, можна змусити систему вимагати складні паролі, заборонити використання USB-пристроїв для зберігання ланних або обмежити доступ до певних налаштувань Windows.

Однією з переваг є, що GPO можна налаштовувати вибірково для різних підрозділів чи пристроїв, адаптуючи політики до конкретних потреб. Крім цього, політики дозволяють включити введення журналів, що допомагає бачити, хто що зробив у системі і оперативно реагувати на потенційні загрози. В цілому, групові політики – це надійний та гнучкий фундамент для захисту всієї мережі [10].

PowerShell є незамінним помічником адміністратора домену AD. Завдяки йому можна автоматизувати рутинні, але критично важливі задачі, такі як: зміну паролів, перевірку журналів, контроль доступу до ресурсів, тощо. Це дозволяє зекономити час і зменшити ризик людських помилок.

PowerShell часто використовується для швидкої діагностики, наприклад, щоб перевірити статус домен-контролерів або зібрати інформацію про підозрілу активність. Крім того, скрипти PowerShell можна запускати регулярно, формуючи звіти про безпеку або виконуючи профілактичні перевірки. Завдяки своїй гнучкості цей інструмент і стає незамінним у повсякденній роботі фахівця з кібербезпеки [11].

2.3 Впровадження політик безпеки для захисту AD:

2.3.1 Парольна політика

Складні паролі користувачів і в тому числі адміністраторів домену є одним з перших бар'єрів на шляху до компрометації доступу до доменної системи. Політика паролів у домені AD встановлюється через GPO – зазвичай

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

через Default Domain Policy. Основні параметри налаштування парольної політики в домені представлені в табл. 2.2:

Таблиця 2.2

Основні параметри парольної політики в домені

Параметр	Конфігурація політики за рекомендаціями стандартів безпеки
Ведення журналу паролів (Enforce password history)	24 останніх паролі зберігаються, щоб уникнути повторного використання паролів
Максимальний термін дії пароля (Maximum password age)	Через 90 днів користувач зобов'язаний змінити пароль – це забезпечує регулярне оновлення доступу
Мінімальний термін життя пароля (Minimum password age)	1 день. Блок багаторазової зміни паролю в короткий термін, щоб уникнути обходу історії паролів.
Мінімальна довжина пароля (Minimum password length)	Рекомендація про встановлення паролю, в якому не менше 12 символів.
Пароль повинен відповідати вимогам складності (Password must meet complexity requirements)	Пароль повинен містити літери верхнього та нижнього регістру, цифри та спецсимволи.
Зберігати паролі, використовуючи оборотне шифрування (Store passwords using reversible encryption)	Вмикається лише у виключних випадках, бо знижує безпеку.

2.3.2 Політика блокування облікових записів

Політика блокування облікових записів є одним із ключових механізмів забезпечення безпеки в доменних середовищах на базі Active Directory. Вона дозволяє захистити інфраструктуру від атак типу brute-force — спроб підбору пароля шляхом багаторазового введення різних комбінацій.

Ідея полягає в тому, що після кількох невдалих спроб автентифікації обліковий запис автоматично блокується на певний період часу. Це значно ускладнює або повністю зупиняє спроби злому паролів, особливо якщо зловмисник використовує автоматизовані інструменти.

Завдяки гнучкості налаштувань адміністратор може адаптувати політику блокування відповідно до потреб організації — балансуючи між рівнем захисту та зручністю для користувачів.

У таблиці 2.3 наведено основні параметри, які зазвичай налаштовуються для реалізації політики блокування.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні параметри політики блокування облікових записів

Параметр	Опис
Account lockout threshold	Кількість допустимих невдалих спроб входу до блокування
Account lockout duration	Час, протягом якого обліковий запис залишається заблокованим
Reset account lockout counter after	Період, після якого лічильник невдалих спроб скидається

2.3.3 Аудит безпеки

Аудит – це «очі» системного адміністратора. Завдяки налаштуванню журналів подій у Active Directory можна в реальному часі бачити, що відбувається в системі: хто заходив, хто намагався підібрати пароль, чи вносились зміни в політики безпеки. Це важливо не лише для реагування на інциденти, а й для профілактики, щоб помічати підозрілу активність ще до того, як станеться щось критичне.

Для ефективного моніторингу безпеки в середовищі Windows необхідно розуміти, як працює Windows Event Viewer. Саме через нього адміністратор отримує звіти про найважливіші події — від запуску служб до невдалих спроб входу. Цей інструмент — основа для аналізу дій користувачів, служб і можливих загроз.

До ключових журналів подій належать: System, Application, Security, Setup та Forwarded Events. Їх призначення наведено у таблиці 2.3.

Таблиця 2.4

Ключові журнали подій у Windows Event Viewer

Журнал подій	Призначення
Security	Входи/виходи в систему, невдалі спроби авторизації
Application	Фіксує події, згенеровані прикладними програмами, наприклад, помилки запуску або збої у роботі ПЗ
System	Події на рівні ОС – інформація про роботу служб, драйверів, збоїв тощо.
Setup	Відображає події, що виникають під час інсталяції ОС Windows
Forwarded Events	Містить події, переслані з інших комп'ютерів мережі

2.3.4 Обмеження адміністративного доступу

Мінімум прав – максимум безпеки. Це один із головних принципів захисту в корпоративному середовищі. Адміністративні облікові записи мають використовуватись виключно тоді, коли справді необхідно виконати завдання з розширеними повноваженнями. Для повсякденної роботи, включно з адміністративною, доцільно застосовувати обмежені облікові записи — без прав, які не потрібні в конкретний момент. Це знижує ризики випадкового або зловмисного втручання в критичні компоненти системи. Окрім цього, доступ до критичних складових системи має бути додатково захищений. Для цього можна використовувати сегментування мережі, протоколи безпеки тощо.

2.3.5 Інші політики безпеки в Active Directory

Окрім базових політик, таких як політика паролів, блокування облікових записів чи аудит, у корпоративному середовищі Active Directory важливу роль відіграють інші обмежувальні політики. Вони дозволяють точково впливати на поведінку системи, обмежити доступ до критичних функцій, керувати використанням зовнішніх носіїв та запуском додатків. Ці політики реалізуються через механізми групових політик (GPO) і заплановані до впровадження на подальших етапах захисту мережі. Вони відповідають принципу мінімальних привілеїв та дозволяють зменшити вірогідність помилкових або зловмисних дій з боку користувачів. У таблиці 2.5 наведено основні додаткові політики безпеки.

Таблиця 2.5

Додаткові політики безпеки, заплановані до реалізації в AD

Політика	Опис	Призначення
Заборона запуску PowerShell	Через AppLocker заблоковано запуск powershell.exe та pwsh.exe	Унеможливлення запуску шкідливих скриптів або втручання в систему
Блокування USB-пристроїв для зберігання даних	Через політику Device Installation обмежено використання знімних носіїв	Захист від витоку даних або зараження шкідливим ПЗ
Обмеження запуску EXE-додатків	Дозволено запуск лише програм з каталогу C:\Program Files	Контроль за дозволеними програмами та уникнення запуску підозрілих

Автоматичне блокування екрана	Після 5 хвилин бездіяльності вмикається блокування	Захист сесії користувача у разі його відсутності
Вхід лише членів певної групи	Локальний вхід дозволено лише користувачам із певної AD-групи	Обмеження доступу до станцій РАВ лише для уповноважених

2.4 Налаштування корпоративної мережі

На основі теоретичних принципів захисту Active Directory та вимог до побудови безпечної інфраструктури було спроектовано макет корпоративної мережі з урахуванням сегментування, резервування та доступу до ключових служб. Архітектура побудована таким чином, щоб забезпечити ізольовану взаємодію між окремими підмережами (VLAN), централізоване адміністрування та гнучкість у налаштуванні політик безпеки.

Схематичне представлення створеної мережевої топології наведено на рисунку 2.4

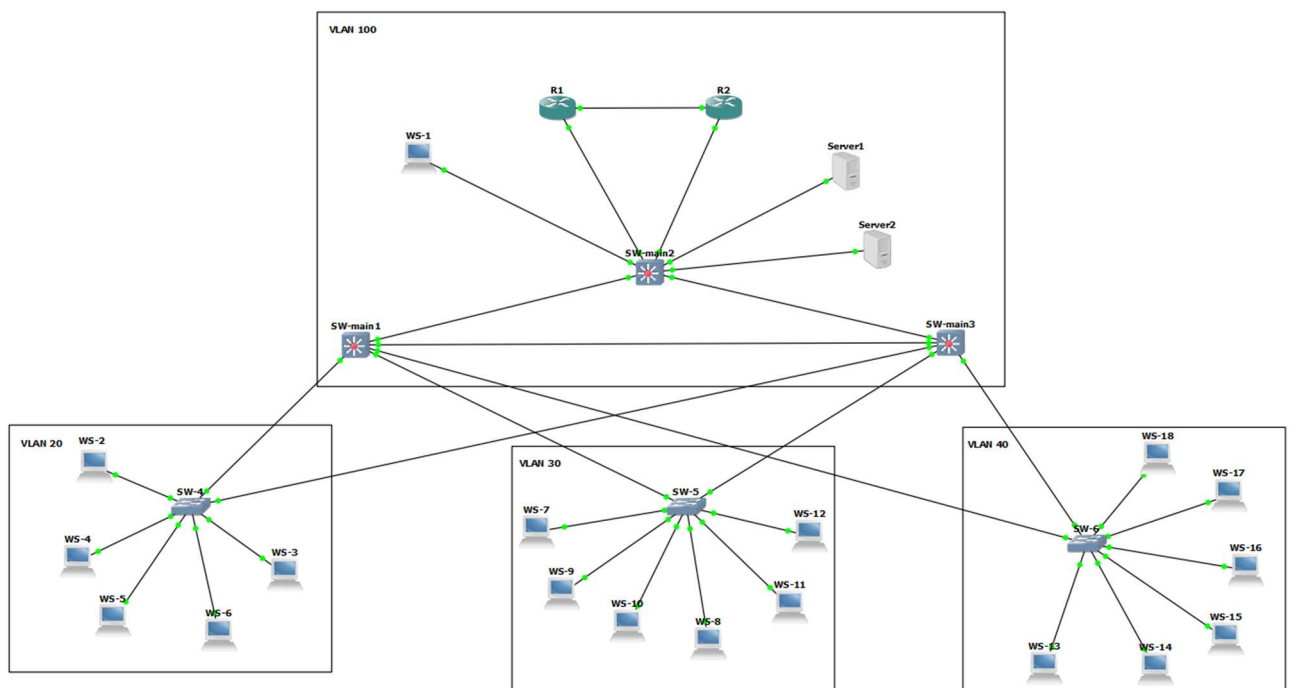


Рисунок 2.4 – Проєкт мережі

У рамках проєктування корпоративної мережі важливою складовою стало логічне розділення трафіку за допомогою VLAN. Це дозволяє досягти кращого контролю доступу, підвищити рівень безпеки та оптимізувати

керуваність інфраструктури. У таблиці 2.5. наведено список VLAN, що використовуються у мережі, із відповідними IP-підмережами.

Таблиця 2.5

Перелік VLAN та їх IP-адресація

VLAN	Підмережа
VLAN 100	192.168.19.0/28
VLAN 20	192.168.20.0/24
VLAN 30	192.168.30.0/24
VLAN 40	192.168.40.0/24

Крім логічної структури, для побудови мережі важливо також коректно організувати фізичні підключення між мережевими пристроями. Нижче у таблиці 2.6 наведено детальну інформацію про підключення елементів корпоративної мережі.

Таблиця 2.6

Параметри фізичних інтерфейсів і підключення між пристроями

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R1	Fa0/0	Маршрутизатор R2	Fa0/0
Маршрутизатор R1	Fa1/0	Комутатор SW-main2	E2/0
Маршрутизатор R2	Fa0/0	Маршрутизатор R1	Fa0/0
Маршрутизатор R2	Fa1/0	Комутатор SW-main2	E1/3
Комутатор SW-main1	E0/0	Комутатор SW-main2	E1/1
Комутатор SW-main1	E0/1	Комутатор SW-4	E0/0
Комутатор SW-main1	E0/2	Комутатор SW-5	E0/0
Комутатор SW-main1	E0/3	Комутатор SW-main3	E0/3
Комутатор SW-main1	E1/0	Комутатор SW-6	E0/1
Комутатор SW-main2	E0/0	Сервер Server1	E0
Комутатор SW-main2	E0/1	Сервер Server1	E1
Комутатор SW-main2	E0/2	Сервер Server2	E0
Комутатор SW-main2	E0/3	Сервер Server2	E1

Комутатор SW-main2	E1/0	Р. Станція WS-1	E0
Комутатор SW-main2	E1/1	Комутатор SW-main1	E0/0
Комутатор SW-main2	E1/2	Комутатор SW-main3	E0/0
Комутатор SW-main2	E1/3	Маршрутизатор R2	Fa1/0
Комутатор SW-main2	E2/0	Маршрутизатор R1	Fa1/0
Комутатор SW-main3	E0/0	Комутатор SW-main2	E1/2
Комутатор SW-main3	E0/1	Комутатор SW-6	E0/0
Комутатор SW-main3	E0/2	Комутатор SW-5	E0/1
Комутатор SW-main3	E0/3	Комутатор SW-main1	E0/3
Комутатор SW-main3	E1/0	Комутатор SW-4	E0/1

У таблиці 2.7 представлено конкретні IP-адреси, призначені кожному елементу мережі. Зокрема, маршрутизатори R-1 і R-2 мають інтерфейси у підмережі VLAN100, що дозволяє реалізувати резервування шлюзу за допомогою HSRP. Комутатори SW-main1, SW-main2 та SW-main3 мають адреси управління у VLAN100 для віддаленого адміністрування. Сервер з Active Directory (Server1) також підключено до цієї VLAN, що забезпечує централізований контроль та розгортання політик.

Таблиця 2.7

Адресація мережі

Мережа/пристрій	Інтерфейс/Мережевий адаптер/Шлюз	IP-адреса	Маска
VLAN100 Management	-	192.168.19.0	255.255.255.240
R-1	Fa1/0.100	192.168.19.1	255.255.255.240
R-2	Fa1/0.100	192.168.19.2	255.255.255.240
SW-main1	Vlan100	192.168.19.4	255.255.255.240
SW-main2	Vlan100	192.168.19.6	255.255.255.240
SW-main3	Vlan100	192.168.19.7	255.255.255.240

Продовження таблиці 2.7

Windows сервер Server1	Мережевий адаптер	192.168.19.12	255.255.255.240
	Шлюз за замовч.	192.168.19.1	255.255.255.240
Windows сервер Server2	Мережевий адаптер	192.168.19.13	255.255.255.240
	Шлюз за замовч.	192.168.19.1	255.255.255.240
WS-1	Мережевий адаптер	192.168.19.11	255.255.255.240
	Шлюз за замовч.	192.168.19.1	255.255.255.240
R-1	Fa0/0	192.168.255.1	255.255.255.252
R-2	Fa0/0	192.168.255.2	255.255.255.252
VLAN20	-	192.168.20.0	255.255.255.0
R-1	Fa1/0.20	192.168.20.1	255.255.255.0
R-2	Fa1/0.20	192.168.20.2	255.255.255.0
SW-4	Vlan20	192.168.20.8	255.255.255.0
WS-2 – WS-6	Мережевий адаптер	192.168.20.10-14	255.255.255.0
	Шлюз за замовч.	192.168.20.1	255.255.255.0
	Шлюз за замовч.	192.168.20.1	255.255.255.0
VLAN30	-	192.168.30.0	255.255.255.0
R-1	Fa1/0.30	192.168.30.1	255.255.255.0
R-2	Fa1/0.30	192.168.30.2	255.255.255.0
SW-5	Vlan30	192.168.30.8	255.255.255.0
WS-7 – WS-12	Мережевий адаптер	192.168.30.12-17	255.255.255.0
	Шлюз за замовч.	192.168.30.1	255.255.255.0
VLAN40	-	192.168.40.0	255.255.255.0
R-1	Fa1/0.40	192.168.40.1	255.255.255.0
R-2	Fa1/0.40	192.168.40.2	255.255.255.0
SW-6	Vlan40	192.168.40.8	255.255.255.0
WS-13 – WS-18	Мережевий адаптер	192.168.40.18-23	255.255.255.0
	Шлюз за замовч.	192.168.40.1	255.255.255.0

Налаштування маршрутизатора R1 та R2. Для забезпечення безперебійного доступу до мережевих ресурсів у мережі було впроваджено протокол HSRP. Його суть полягає в тому, що два маршрутизатори R1 та R2 працюють як основний та резервний шлюз.

Пристрій користувача бачить лише одну IP-адресу шлюзу. Основний маршрутизатор обробляє трафік у нормальному режимі, але якщо він вийде з ладу, автоматично активується резервний маршрутизатор.

Таким чином, HSRP дозволяє автоматично перемикає маршрутизацію без перерви в роботі мережі, що є важливим для надійної роботи.

На R1 використовується більший пріоритет і він стає активним шлюзом.

Конфігурацію HSRP та приклади налаштувань на маршрутизаторах зображено на рисунках 2.5 та 2.6.

```

R1
R1(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#interface FastEthernet1/0.100
R1(config-subif)# encapsulation dot1Q 100
R1(config-subif)# ip address 192.168.19.1 255.255.255.240
R1(config-subif)# standby 100 ip 192.168.19.3
R1(config-subif)# standby 100 priority 110
R1(config-subif)# standby 100 preempt
R1(config-subif)# description VLAN 100 - Management
R1(config-subif)#exit

```

Рисунок – 2.5 Конфігурація маршрутизатора R1 для VLAN 100 із реалізацією HSRP

```

R1(config)#interface FastEthernet1/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# standby 20 ip 192.168.20.10
R1(config-subif)# standby 20 priority 110
R1(config-subif)# standby 20 preempt
R1(config-subif)# description VLAN 20 - Workstations
R1(config-subif)#exit
R1(config)#interface FastEthernet1/0.30
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.30.1 255.255.255.0
R1(config-subif)# standby 30 ip 192.168.30.10
R1(config-subif)# standby 30 priority 110
R1(config-subif)# standby 30 preempt
R1(config-subif)# description VLAN 30 - Engineering
R1(config-subif)#exit
R1(config)#interface FastEthernet1/0.40
R1(config-subif)# encapsulation dot1Q 40
R1(config-subif)# ip address 192.168.40.1 255.255.255.0
R1(config-subif)# standby 40 ip 192.168.40.10
R1(config-subif)# standby 40 priority 110
R1(config-subif)# standby 40 preempt
R1(config-subif)# description VLAN 40 - Finance
R1(config-subif)#exit
R1(config)#interface FastEthernet0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 192.168.255.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)#interface FastEthernet1/0
R1(config-if)#no shutdown
R1(config-if)#end

```

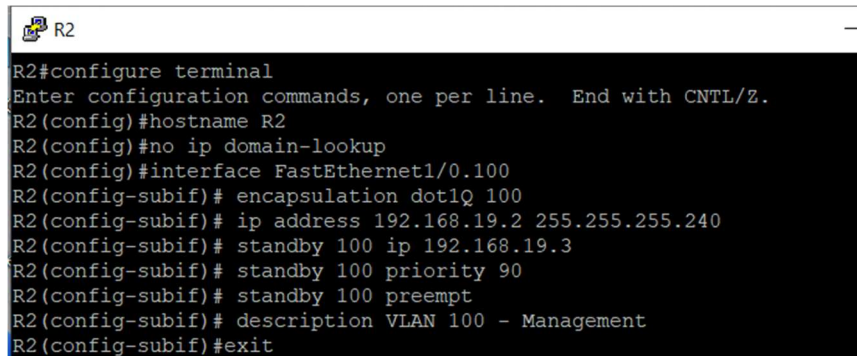
Рисунок – 2.6 Конфігурація маршрутизатора R1 для VLAN 20, 30 та 40 з підтримкою HSRP

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування R2 як резервного маршрутизатора.

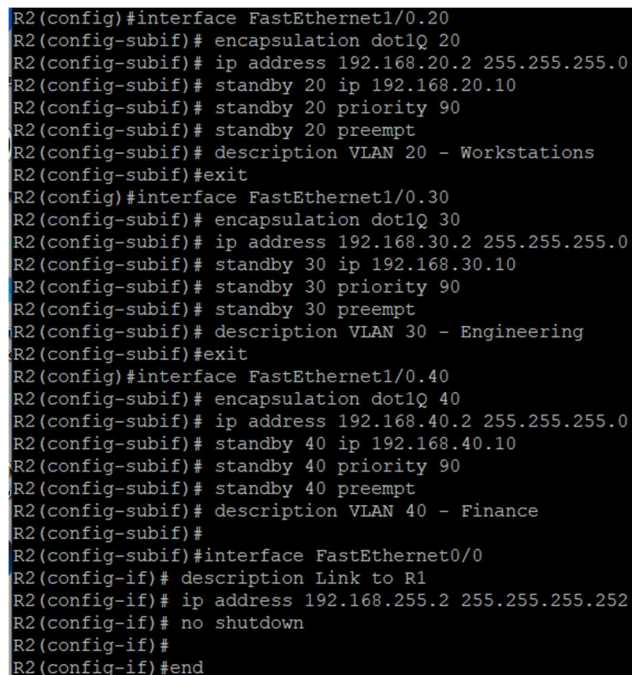
Маршрутизатор R2 налаштовано як резервний у межах протоколу HSRP. У нормальному режимі він перебуває в пасивному стані, очікуючи виходу з ладу активного вузла R1. У разі відмови R1, R2 автоматично перебирає на себе функції шлюзу для VLAN, забезпечуючи безперервність маршрутизації.

Рисунки 2.7 та 2.8 демонструють відповідну конфігурацію R2, що дозволяє забезпечити відмовостійкість мережі.



```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#interface FastEthernet1/0.100
R2(config-subif)# encapsulation dot1Q 100
R2(config-subif)# ip address 192.168.19.2 255.255.255.240
R2(config-subif)# standby 100 ip 192.168.19.3
R2(config-subif)# standby 100 priority 90
R2(config-subif)# standby 100 preempt
R2(config-subif)# description VLAN 100 - Management
R2(config-subif)#exit
```

Рисунок 2.7 – Налаштування резервного маршрутизатора R2 для VLAN 100 з HSRP



```
R2(config)#interface FastEthernet1/0.20
R2(config-subif)# encapsulation dot1Q 20
R2(config-subif)# ip address 192.168.20.2 255.255.255.0
R2(config-subif)# standby 20 ip 192.168.20.10
R2(config-subif)# standby 20 priority 90
R2(config-subif)# standby 20 preempt
R2(config-subif)# description VLAN 20 - Workstations
R2(config-subif)#exit
R2(config)#interface FastEthernet1/0.30
R2(config-subif)# encapsulation dot1Q 30
R2(config-subif)# ip address 192.168.30.2 255.255.255.0
R2(config-subif)# standby 30 ip 192.168.30.10
R2(config-subif)# standby 30 priority 90
R2(config-subif)# standby 30 preempt
R2(config-subif)# description VLAN 30 - Engineering
R2(config-subif)#exit
R2(config)#interface FastEthernet1/0.40
R2(config-subif)# encapsulation dot1Q 40
R2(config-subif)# ip address 192.168.40.2 255.255.255.0
R2(config-subif)# standby 40 ip 192.168.40.10
R2(config-subif)# standby 40 priority 90
R2(config-subif)# standby 40 preempt
R2(config-subif)# description VLAN 40 - Finance
R2(config-subif)#
R2(config-subif)#interface FastEthernet0/0
R2(config-if)# description Link to R1
R2(config-if)# ip address 192.168.255.2 255.255.255.252
R2(config-if)# no shutdown
R2(config-if)#
R2(config-if)#end
```

Рисунок 2.8 – Конфігурація маршрутизатора R2 для VLAN 20, 30 та 40 з HSRP

Також налаштуємо службовий зв'язок між маршрутизаторами, який наведено на рисунку 2.9. Аналогічно було налаштовано R2.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R1
R1(config)#interface FastEthernet0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 192.168.255.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)#

```

Рисунок 2.9 – Налаштування інтерфейсу FastEthernet0/0 на маршрутизаторі R1 для зв’язку з R2

Початкові налаштування комутаторів управління. Приклад налаштувань адресації та створення VLAN представлено на рисунку 2.10. На інших комутаторах управління було впроваджено аналогічні налаштування.

```

SW-main1
SW-main1(config)#hostname SW-main1
SW-main1(config)#no ip domain-lookup
SW-main1(config)#
SW-main1(config)#vlan 100
SW-main1(config-vlan)# name Management
SW-main1(config-vlan)#vlan 20
SW-main1(config-vlan)# name Workstations
SW-main1(config-vlan)#vlan 30
SW-main1(config-vlan)# name Engineering
SW-main1(config-vlan)#vlan 40
SW-main1(config-vlan)# name Finance
SW-main1(config-vlan)#
SW-main1(config-vlan)#interface vlan 100
SW-main1(config-if)# ip address 192.168.19.4 255.255.255.240
SW-main1(config-if)# no shutdown
SW-main1(config-if)#

```

Рисунок 2.10 – Конфігурація комутатора SW-main1: створення VLAN і налаштування керуючої VLAN

Приклад налаштування транкових каналів. Приклад конфігурації транкових каналів наведено на рисунку 2.11.

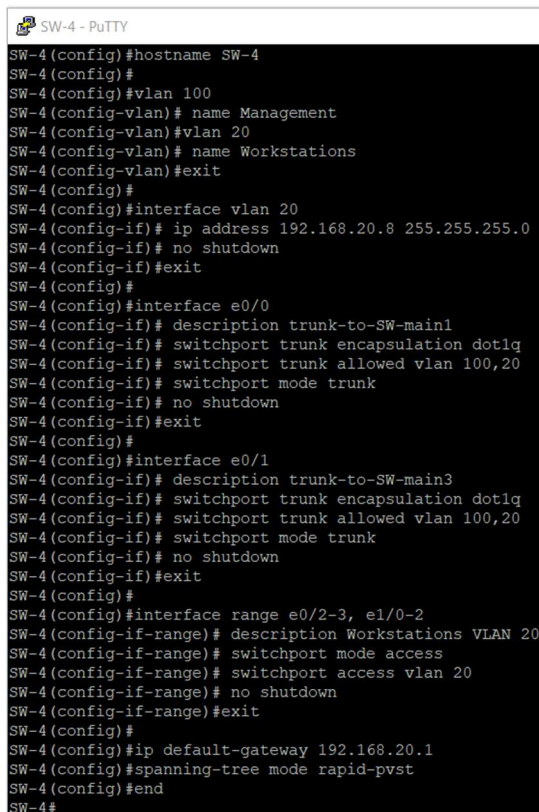
```

SW-main1
SW-main1(config)#interface Ethernet0/0
SW-main1(config-if)# description trunk-to-SW-main2
SW-main1(config-if)# switchport trunk encapsulation dot1q
SW-main1(config-if)# switchport mode trunk
SW-main1(config-if)# switchport trunk allowed vlan 20,30,40,100
SW-main1(config-if)# no shutdown
SW-main1(config-if)#
SW-main1(config-if)#interface Ethernet0/1
SW-main1(config-if)# description trunk-to-SW-4
SW-main1(config-if)# switchport trunk encapsulation dot1q
SW-main1(config-if)# switchport mode trunk
SW-main1(config-if)# switchport trunk allowed vlan 20,100
SW-main1(config-if)# no shutdown
SW-main1(config-if)#
SW-main1(config-if)#interface Ethernet0/2
SW-main1(config-if)# description trunk-to-SW-5
SW-main1(config-if)# switchport trunk encapsulation dot1q
SW-main1(config-if)# switchport mode trunk
SW-main1(config-if)# switchport trunk allowed vlan 30,100
SW-main1(config-if)# no shutdown
SW-main1(config-if)#
SW-main1(config-if)#interface Ethernet0/3
SW-main1(config-if)# description trunk-to-SW-main3
SW-main1(config-if)# switchport trunk encapsulation dot1q
SW-main1(config-if)# switchport mode trunk
SW-main1(config-if)# switchport trunk allowed vlan 20,30,40,100
SW-main1(config-if)# no shutdown
SW-main1(config-if)#
SW-main1(config-if)#interface Ethernet1/0
SW-main1(config-if)# description trunk-to-SW-6
SW-main1(config-if)# switchport trunk encapsulation dot1q
SW-main1(config-if)# switchport mode trunk
SW-main1(config-if)# switchport trunk allowed vlan 40,100
SW-main1(config-if)# no shutdown
SW-main1(config-if)#

```

Рисунок 2.11 – Налаштування транкового з’єднання на SW-main1

Далі налаштовуємо комутатори доступу. Приклад налаштування комутатора із підмережі VLAN20 продемонстровано на рисунку 2.12. Інші комутатори було налаштовано аналогічно, із змінами адрес на відповідні VLAN.



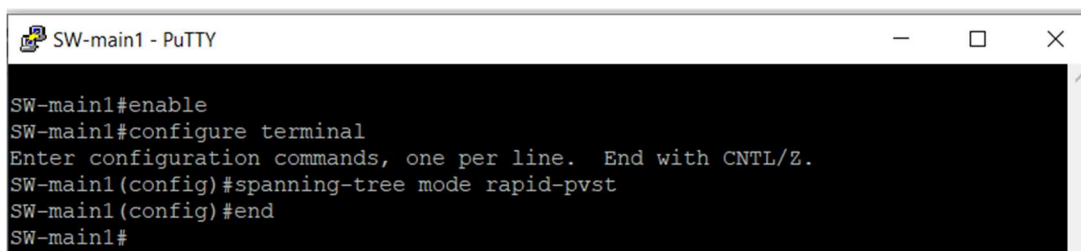
```

SW-4(config)#hostname SW-4
SW-4(config)#
SW-4(config)#vlan 100
SW-4(config-vlan)# name Management
SW-4(config-vlan)#vlan 20
SW-4(config-vlan)# name Workstations
SW-4(config-vlan)#exit
SW-4(config)#
SW-4(config)#interface vlan 20
SW-4(config-if)# ip address 192.168.20.8 255.255.255.0
SW-4(config-if)# no shutdown
SW-4(config-if)#exit
SW-4(config)#
SW-4(config)#interface e0/0
SW-4(config-if)# description trunk-to-SW-main1
SW-4(config-if)# switchport trunk encapsulation dot1q
SW-4(config-if)# switchport trunk allowed vlan 100,20
SW-4(config-if)# switchport mode trunk
SW-4(config-if)# no shutdown
SW-4(config-if)#exit
SW-4(config)#
SW-4(config)#interface e0/1
SW-4(config-if)# description trunk-to-SW-main3
SW-4(config-if)# switchport trunk encapsulation dot1q
SW-4(config-if)# switchport trunk allowed vlan 100,20
SW-4(config-if)# switchport mode trunk
SW-4(config-if)# no shutdown
SW-4(config-if)#exit
SW-4(config)#
SW-4(config)#interface range e0/2-3, e1/0-2
SW-4(config-if-range)# description Workstations VLAN 20
SW-4(config-if-range)# switchport mode access
SW-4(config-if-range)# switchport access vlan 20
SW-4(config-if-range)# no shutdown
SW-4(config-if-range)#exit
SW-4(config)#
SW-4(config)#ip default-gateway 192.168.20.1
SW-4(config)#spanning-tree mode rapid-pvst
SW-4(config)#end
SW-4#
  
```

Рисунок 2.12 – Конфігурація комутатора SW- 4 із налаштуванням VLAN, trunk-з'єднань та керуючого інтерфейсу

Наша мережа побудована таким чином, щоб із VLAN Management до інших підмереж є додаткові зв'язки, що отримуємо в результаті петлювання мережі. Для уникнення петлювання було використано Spanning Tree Protocol (STP) та його вдосконалену версію - RSTP (Rapid Spanning Tree Protocol).

Приклад налаштування протоколу на комутаторі наведено на рисунку 2.13. Аналогічні налаштування були і інших комутаторах мережі.



```

SW-main1#enable
SW-main1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-main1(config)#spanning-tree mode rapid-pvst
SW-main1(config)#end
SW-main1#
  
```

Рисунок 2.13 – Активація протоколу spanning-tree в режимі Rapid PVST на комутаторі SW-main1

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Впровадження SSH у нашій мережі є хорошим засобом захисту, оскільки дозволяє адміністраторам безпечно підключитися до обладнання для налаштування та управління ним. Завдяки шифруванню даних SSH унеможливорює перехоплення паролів і команд зловмисникам. Це особливо актуально для мережі, в якій працює Active Directory.

Налаштування SSH на комутаторі управління SW-main1 наведено на рисунку 2.14. На інших комутаторах відбулось аналогічне налаштування.

```

SW-main1(config)#ip domain-name corp.local
SW-main1(config)#crypto key generate rsa
The name for the keys will be: SW-main1.corp.local
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 0 seconds)

SW-main1(config)#username admin privilege 15 secret Paswd068@
SW-main1(config)#ip ssh version 2
SW-main1(config)#line vty 0 4
SW-main1(config-line)# login local
SW-main1(config-line)# transport input ssh
SW-main1(config-line)#exit
SW-main1(config)#ip ssh time-out 60
SW-main1(config)#ip ssh authentication-retries 3
SW-main1(config)#ip access-list standard SSH_ONLY
SW-main1(config-std-nacl)# permit 192.168.19.0 0.0.0.15
SW-main1(config-std-nacl)#line vty 0 4
SW-main1(config-line)# access-class SSH_ONLY in
SW-main1(config-line)#exit
SW-main1(config)#end
*Jun 18 00:09:09.406: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-main1(config)#end
SW-main1#
  
```

Рисунок 2.14 – Налаштування захищеного доступу до комутатора SW-main1 через SSH

Висновки до другого розділу

У даному розділі було всебічно розглянуто методи та інструменти забезпечення захисту Windows-мережі на базі служби каталогів Active Directory. Здійснено обґрунтований вибір компонентів інфраструктури, включаючи мережеве обладнання — маршрутизатори, L2-комутатори, сервери та робочі станції — з урахуванням потреб корпоративного середовища та вимог до безперебійної роботи.

Також було обґрунтовано вибір версій операційних систем, які використовуються для реалізації домену. Обрано Windows 10 Education як

клієнтську ОС, яка за своїм функціоналом аналогічна версії Enterprise та підтримує ключові засоби керування безпекою. Для серверної частини обґрунтовано використання Windows Server 2019, як оптимального варіанту за критерієм стабільності, сумісності та підтримки основних ролей AD. Порівняння із новішими версіями (Server 2022, 2025) показало, що вибір 2019 року забезпечує всі необхідні можливості при меншій вимогливості до ресурсів віртуального середовища.

Особливу увагу приділено налаштуванню протоколу HSRP для забезпечення високої доступності шлюзу та мінімізації простою в разі відмови основного маршрутизатора. Було спроектовано структуру VLAN, що забезпечує логічне розмежування сегментів мережі за функціональним призначенням та сприяє реалізації політик безпеки. Продемонстровано реалізацію транкових з'єднань для передачі трафіку між мережевими вузлами з підтримкою кількох VLAN.

Окремим підрозділом охоплено аналіз та впровадження політик безпеки у середовищі Active Directory. Розглянуто парольну політику, політику блокування облікових записів, аудит подій, обмеження адміністративного доступу та інші заходи, що відповідають сучасним стандартам інформаційної безпеки. Наведено конкретні параметри політик, рекомендовані стандартами NIST та ISO/IEC 27001/27002.

Було показано принципи практичного застосування моделі найменших привілеїв та сегментування мережі з метою зниження потенційного впливу загроз. Враховано важливість моніторингу подій через системні журнали та значення навчання персоналу в контексті підвищення загального рівня захисту мережевої інфраструктури.

Таким чином, результати цього розділу стали базою для переходу до наступного етапу — реалізації практичних заходів у середовищі віртуалізації, налаштування політик домену та перевірки їх ефективності в умовах моделювання корпоративної мережі.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ ACTIVE DIRECTORY

3.1 Встановлення служби каталогів Active Directory та його налаштування у Windows Server 2019.

На рисунку 3.1 наведено приклад встановлення одного з етапів служби Active Directory.

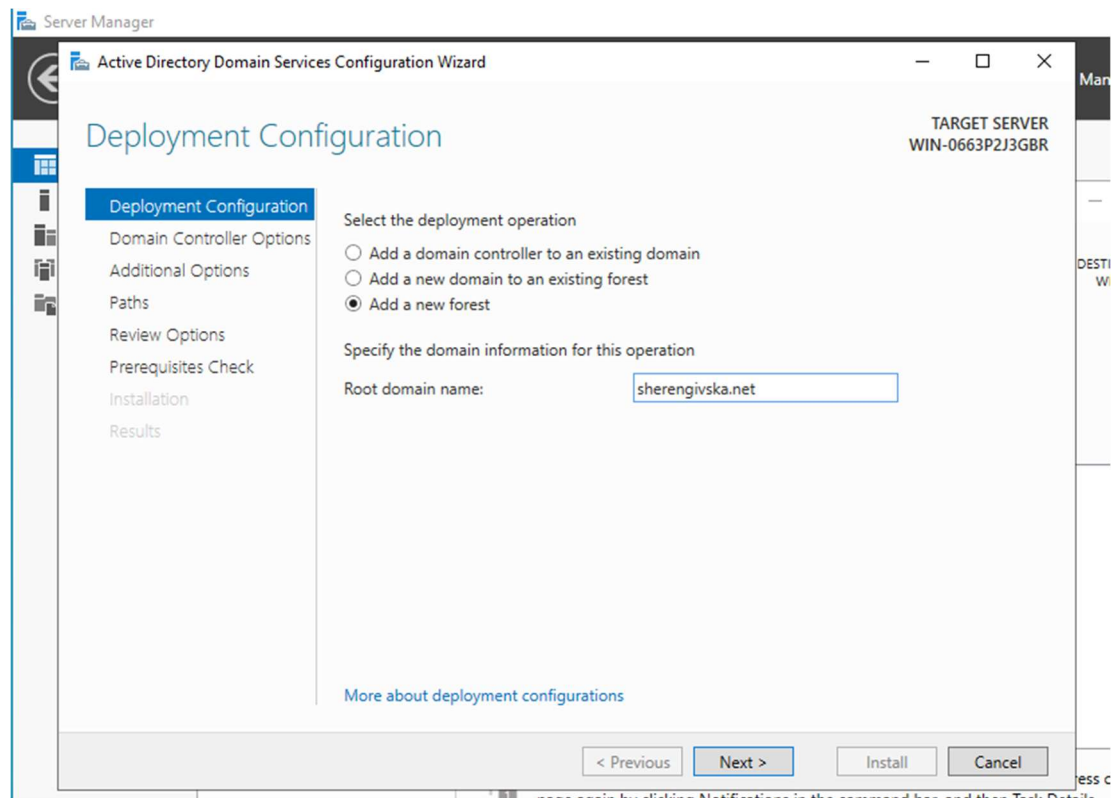


Рисунок – 3.1 Встановлення AD

Щоб підвищити надійність і захищеність мережі, до домену було додано другий контролер. Це означає, що у випадку виходу з ладу основного сервера, другий автоматично бере на себе всі його функції — користувачі цього навіть не помітять.

Такий підхід дозволяє уникнути простоїв у роботі, а також покращує розподіл навантаження — автентифікація та доступ до ресурсів стають швидшими і стабільнішими. Крім того, дані між серверами синхронізуються, тому вся важлива інформація дублюється й завжди залишається доступною.

На рисунку 3.2 наведено другий сервер домену.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

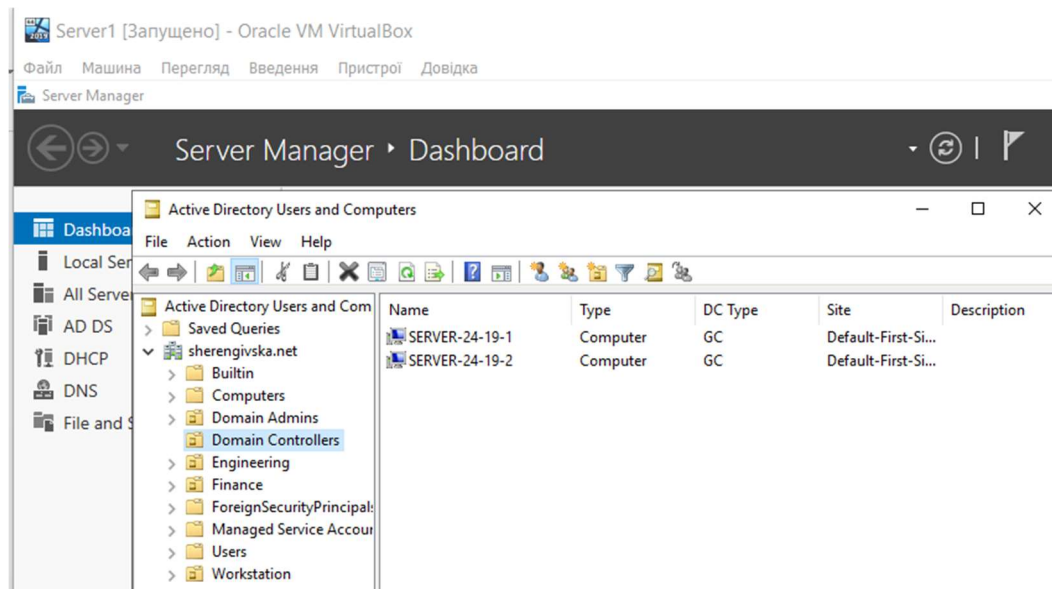


Рисунок 3.2 – Встановлені контролери домену

На рисунку 3.3 представлено результати перевірки реплікації між контролерами домену за допомогою команди `repadmin /replsummary`. Отримані дані свідчать про відсутність помилок, що підтверджує стабільну синхронізацію між серверами.

```
PS C:\Users\Administrator> repadmin /replsummary
Replication Summary Start Time: 2025-06-20 05:07:05

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA          largest delta    fails/total %%   error
SERVER-24-19-1      13m:52s         0 / 5  0
SERVER-24-19-2      13m:41s         0 / 5  0

Destination DSA     largest delta    fails/total %%   error
SERVER-24-19-1      13m:41s         0 / 5  0
SERVER-24-19-2      13m:45s         0 / 5  0
```

Рисунок 3.3 – Реплікація між контролерами домену

Після налаштування домен-контролерів наступним кроком стало приєднання клієнтських машин до домену. Це дозволяє адміністраторам централізовано керувати політиками безпеки, оновленнями та доступом до ресурсів. На рисунках 3.3 – 3.6 показано приклад підключення робочої станції до домену.

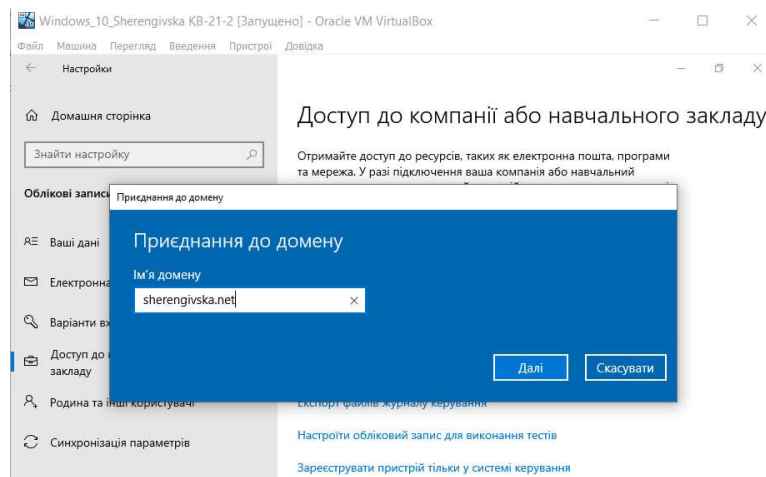


Рисунок 3.4 – Додавання робочої станції до домену

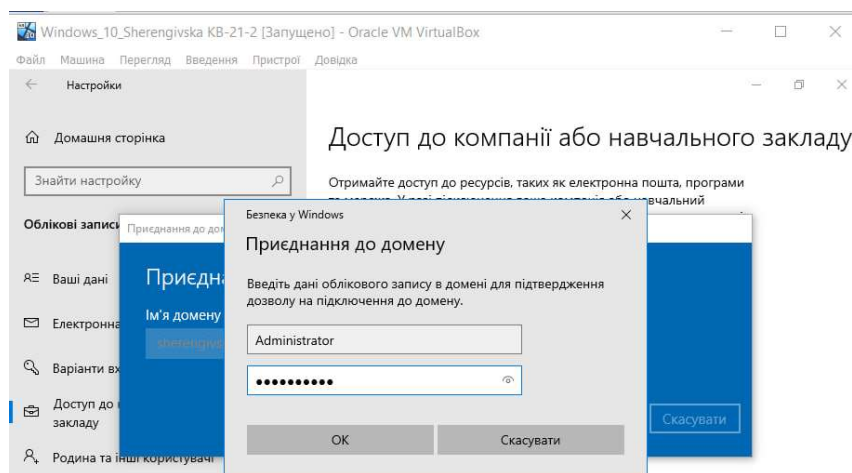


Рисунок 3.5 – Приєднання до домену

Додані робочі станції у домен:

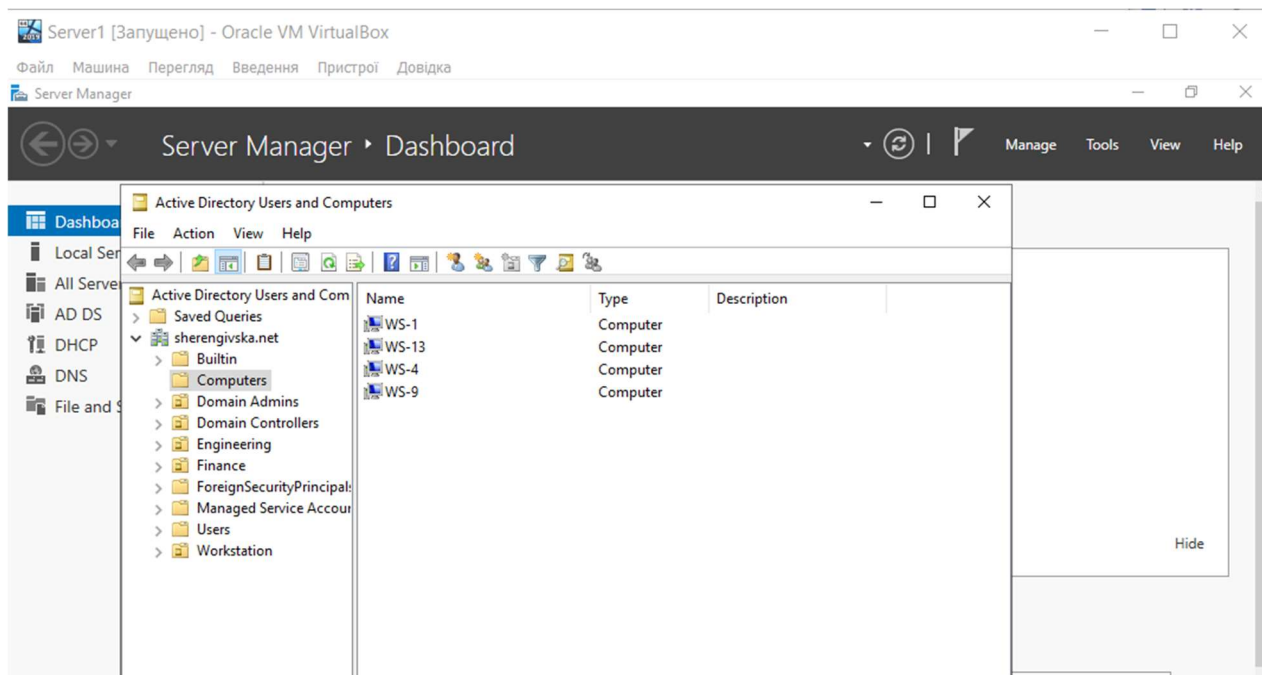


Рисунок 3.6 – Наявність робочих станцій в домені

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

На рисунку 3.7 продемонстровано створену структуру OU в середовищі Active Directory та приклад доданих користувачів.

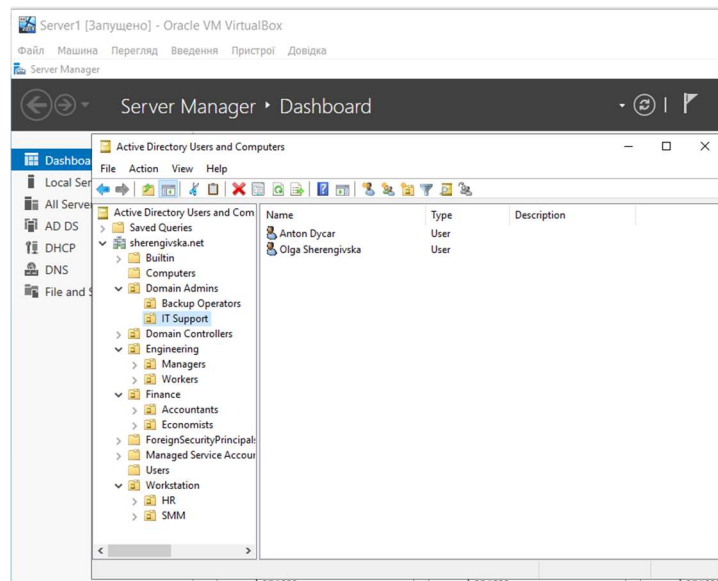


Рисунок 3.7 – Організаційні одиниці та користувачі

3.2 Розробка та впровадження захисту мережі Active Directory

У доменній інфраструктурі реалізовано політики безпеки з урахуванням рекомендацій, викладених у NIST SP 800-53 Rev. 5 та ISO/IEC 27002:2022. Як зазначено в NIST SP 800-53, що організація визначає вимоги до довжини, складності та періодичної зміни автентифікаторів [12], а в ISO 27002:2022 (контроль 5.17) наголошено на необхідності впровадження заходів для захисту автентифікаційної інформації, включаючи історію паролів та блокування облікових записів після невдалих спроб входу [13].

Дані підходи наведено на рисунку 3.8, 3.9 і дозволяють зменшити ризик компрометації облікових даних, унеможливити автоматичний підбір пароля та загалом підвищити рівень захисту автентифікації користувачів у мережі.

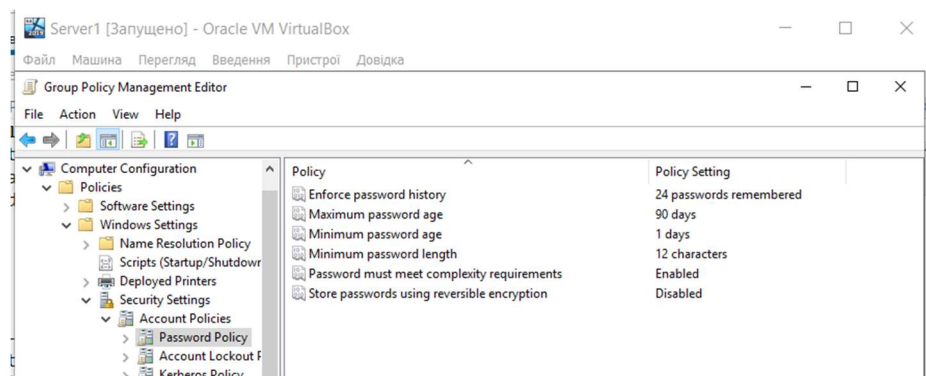


Рисунок 3.8 – Налаштування парольної політики

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

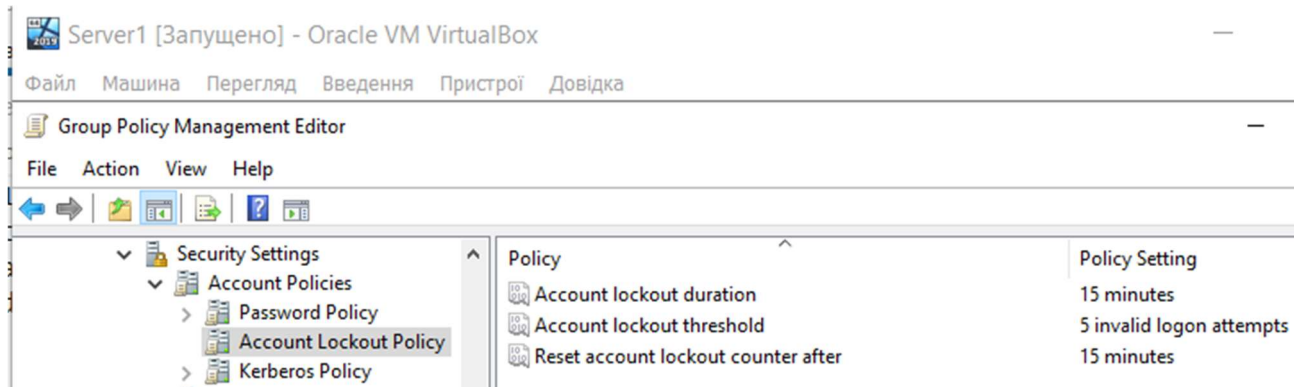


Рисунок 3.9 – Налаштування політик блокування облікових записів

На рисунку 3.10 наведено налаштування політики Kerberos, що відповідають рекомендаціям Microsoft щодо забезпечення безпеки автентифікації в доменних середовищах

У документації наголошується, що час дії квитків (ticket lifetime) має бути достатньо коротким, щоби зменшити ймовірність успішної атаки в разі викрадення облікових даних. Наприклад, параметр Maximum lifetime for user ticket зазвичай встановлюється на рівні 10 годин, що обмежує вікно для зломисника у випадку компрометації сеансу.

Крім того, Maximum lifetime for service ticket за замовчуванням становить 600 хвилин (10 годин), що забезпечує збалансовану тривалість для службових доступів без надмірного ризику.

Важливою є також синхронізація годинників між клієнтами й контролерами домену: параметр Maximum tolerance for computer clock synchronization обмежує цю різницю до 5 хвилин, що є критичним для запобігання відмовам автентифікації [14].

Таке конфігурування відповідає загальним принципам захисту від атак типу Pass-the-Ticket або Replay-атаки, зменшуючи термін дії вкрадених автентифікаторів та посилюючи надійність усього процесу авторизації у мережі.

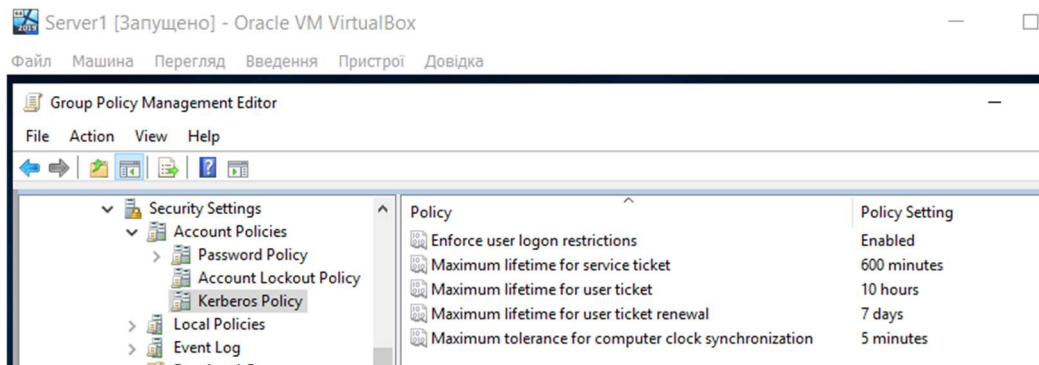


Рисунок 3.10 – Налаштування Kerberos

Щоб уникати ситуацій, коли один адміністратор має надто багато повноважень, у домені було налаштовано делегування доступу для адміністратора. Тепер окремі користувачі можуть керувати лише тим, що їм дійсно потрібно. Це дозволяє розділити відповідальність і зменшити ризик випадкових або навмисних помилок. Налаштування обмеження для Stepan Kokotuk наведено на рисунку 3.11.

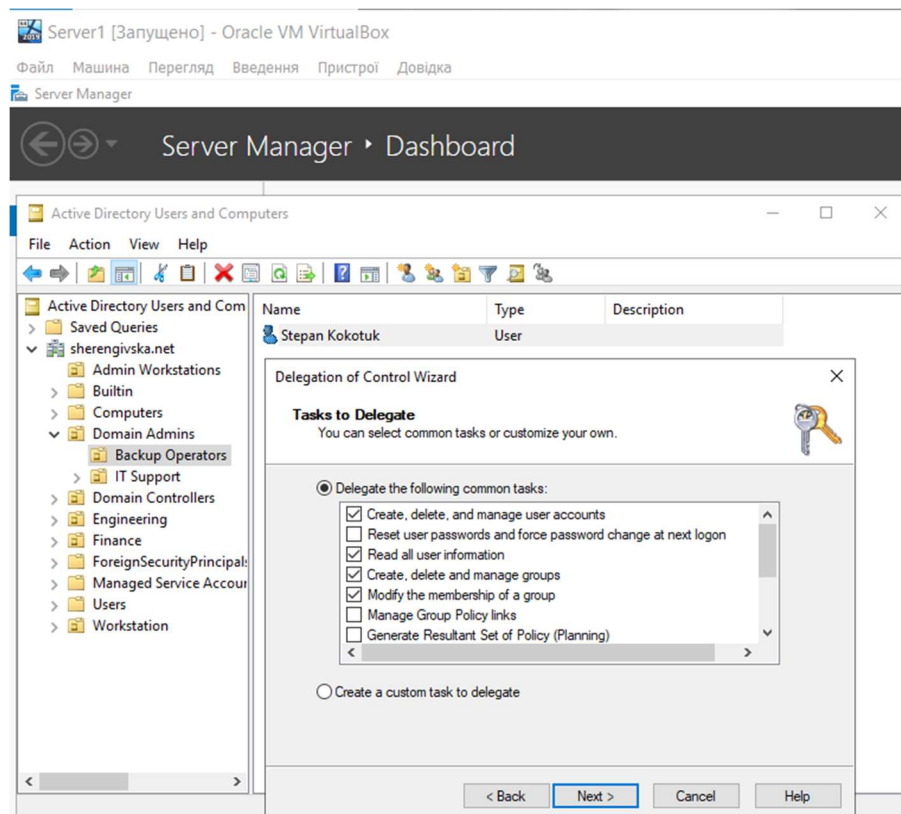


Рисунок 3.11 – Введення обмежених привілеїв для адміністратора

На рисунку 3.12 наведено впровадження дозволу на вхід лише з визначених комп'ютерів, що підвищує контроль доступу та зменшує ризик несанкціонованого використання облікових записів.

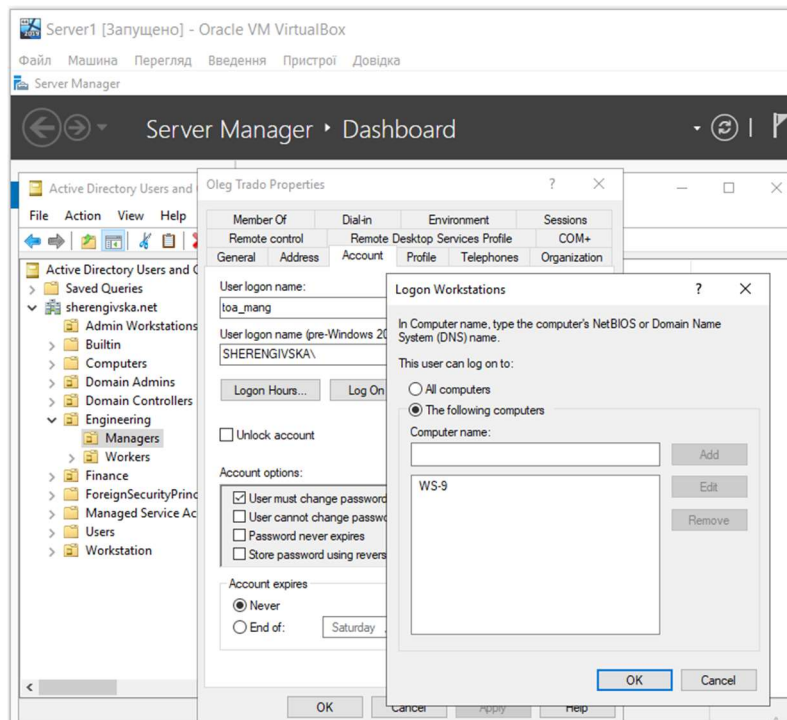


Рисунок 3.12 – Дозвіл на вхід до відповідного комп'ютера

Було створено теку, для відповідної групи користувачів та обмежено доступу до неї. Групі chief and deputy accountant надано повний контроль над текою Finance. Налаштування наведено на рисунку 3.13.

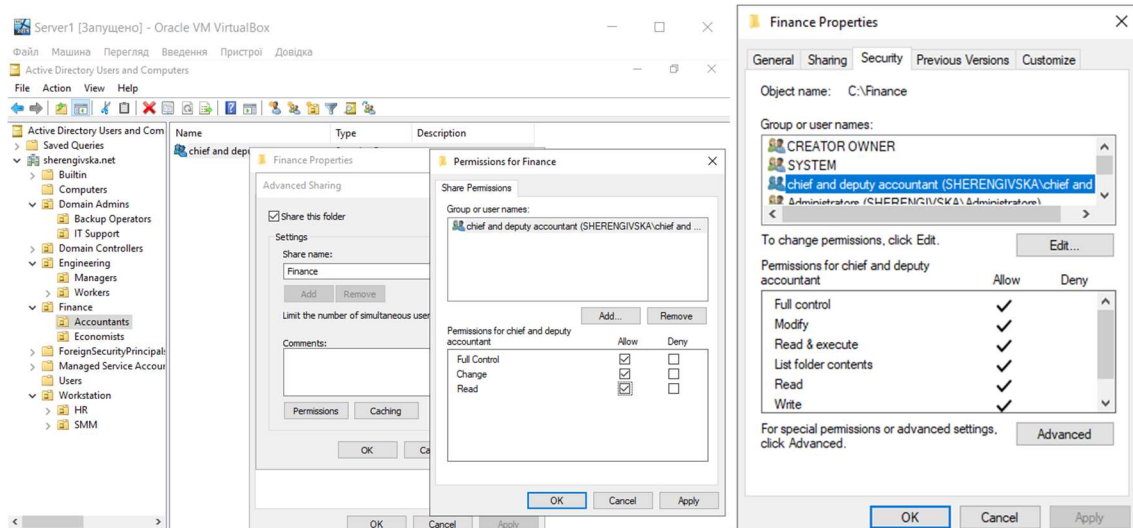


Рисунок 3.13 – Дозвіл для певних груп

Політика заборони використання USB-пристроїв для зберігання даних застосована до організаційних одиниць та діє на всіх її користувачів через загальне фільтрування Authenticated Users. Дана заборона та поширення на користувачів наведено на рисунках 3.14 – 3.15.

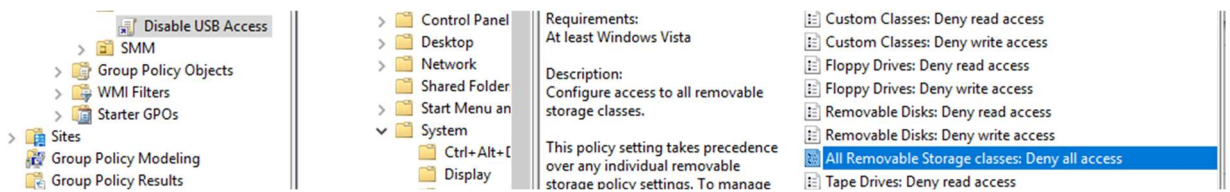


Рисунок 3.14 – Заборона використання USB-пристроїв для зберігання даних

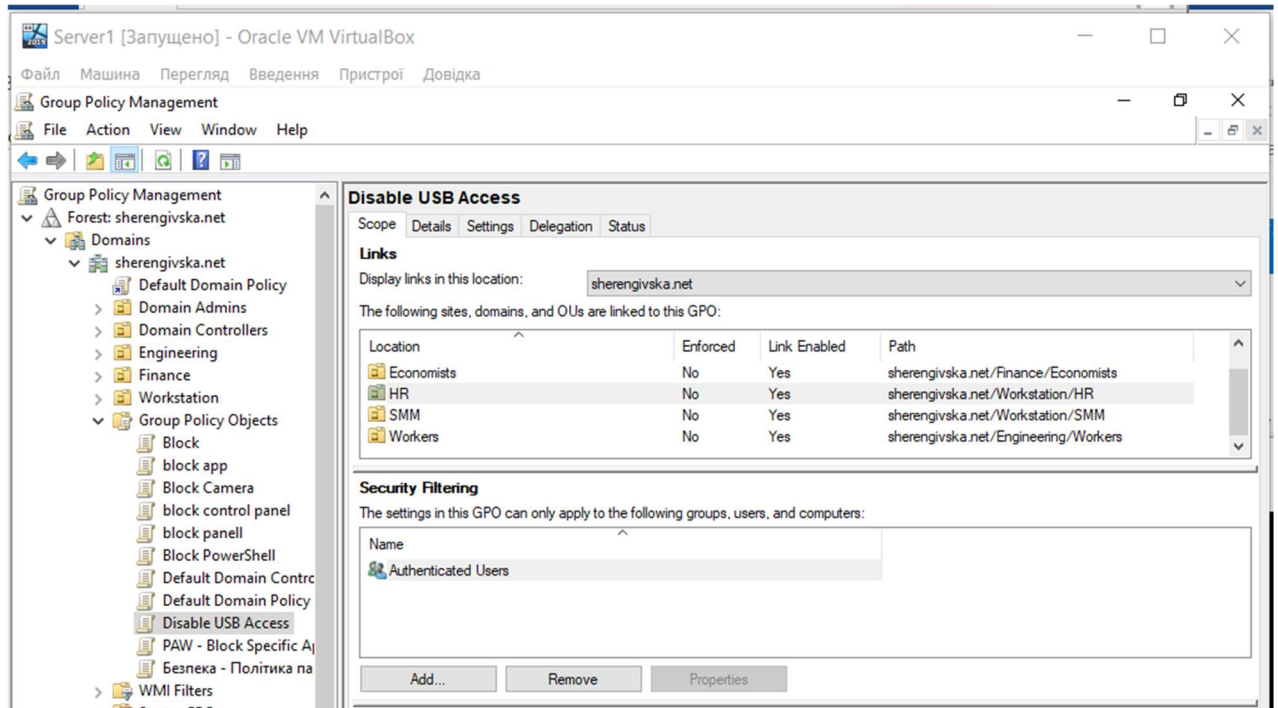


Рисунок 3.15 – Додавання організаційних одиниць до заборони

Обмеження запуску програм. Дозволи на запуск лише системних застосунків та 7-Zip наведено на рисунку 3.16. Це знижує ризик запуску стороннього чи шкідливого ПЗ.

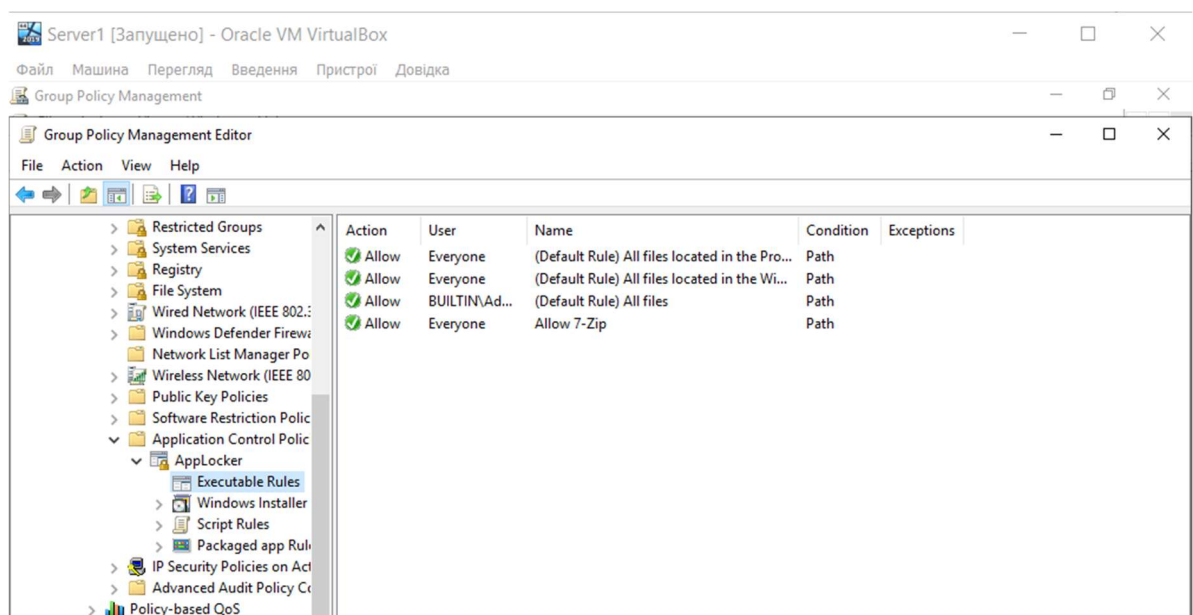


Рисунок 3.16 – Впровадження обмеження

PoweShell було заблоковано для користувачів у ключових підрозділах, що показано на рисунках 3.17 та 3.18. Це обмежує можливість виконання скриптів і адміністративних команд, що підвищує загальний рівень безпеки.

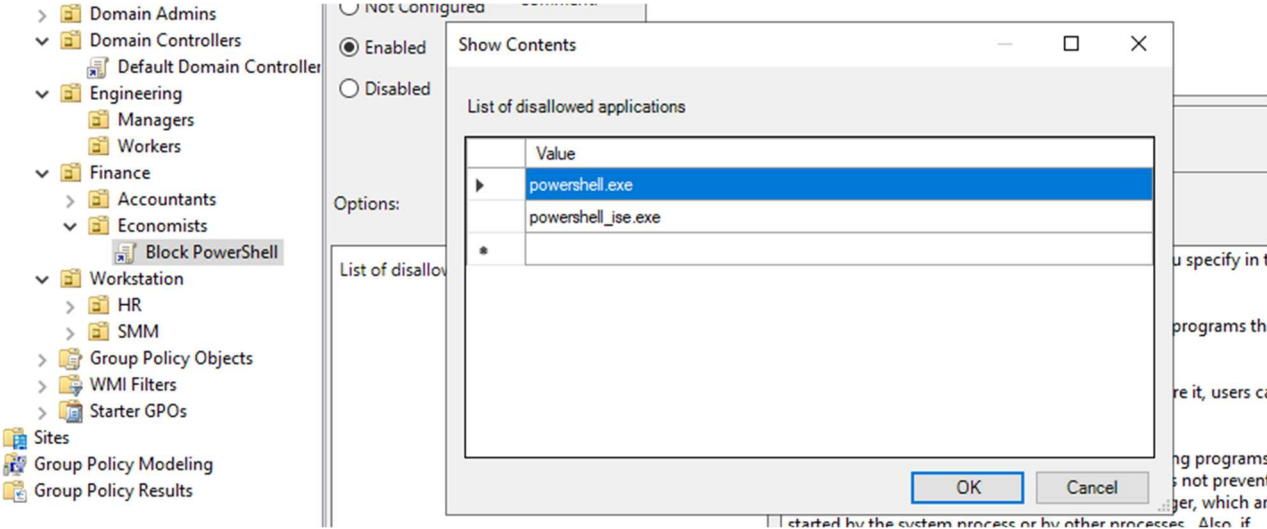


Рисунок 3.17 – Список заборонених програм

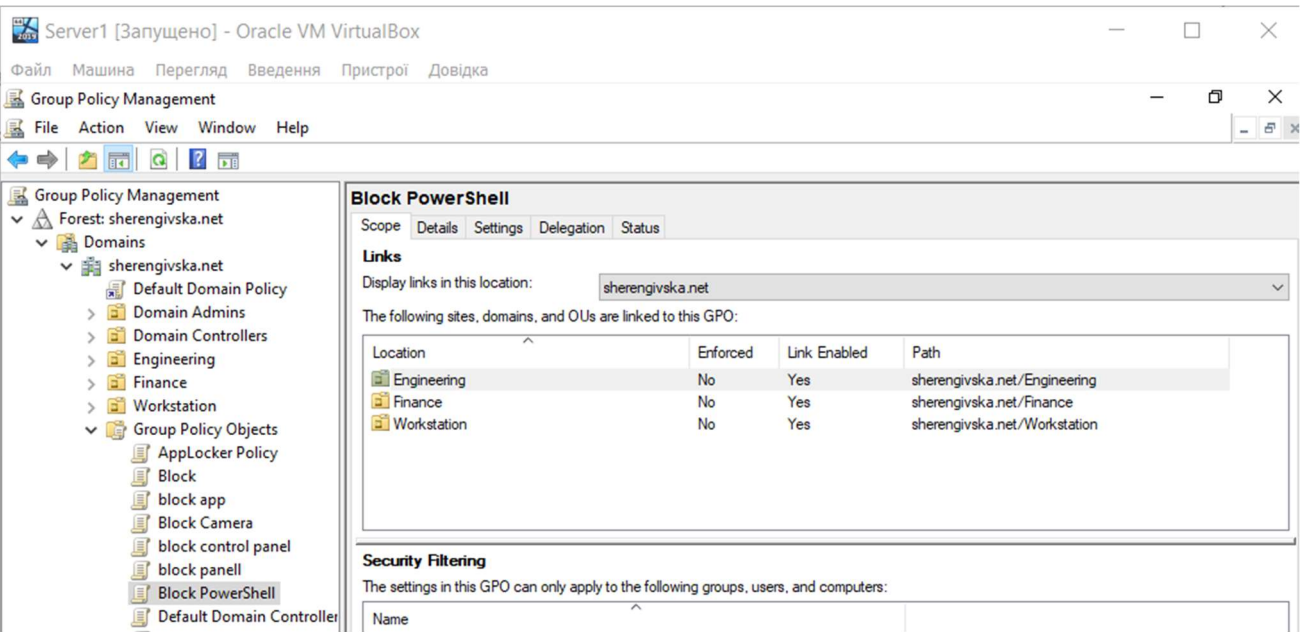


Рисунок 3.18 – Вибір користувачів, на яких поширюється заборона

Активовано автоматичне блокування екрана після 5 хвилин бездіяльності. Це запобігає доступу до системи, якщо користувач залишив робоче місце без блокування сеансу. На рисунках 3.19 – 3.20 представлено налаштування даної політики.

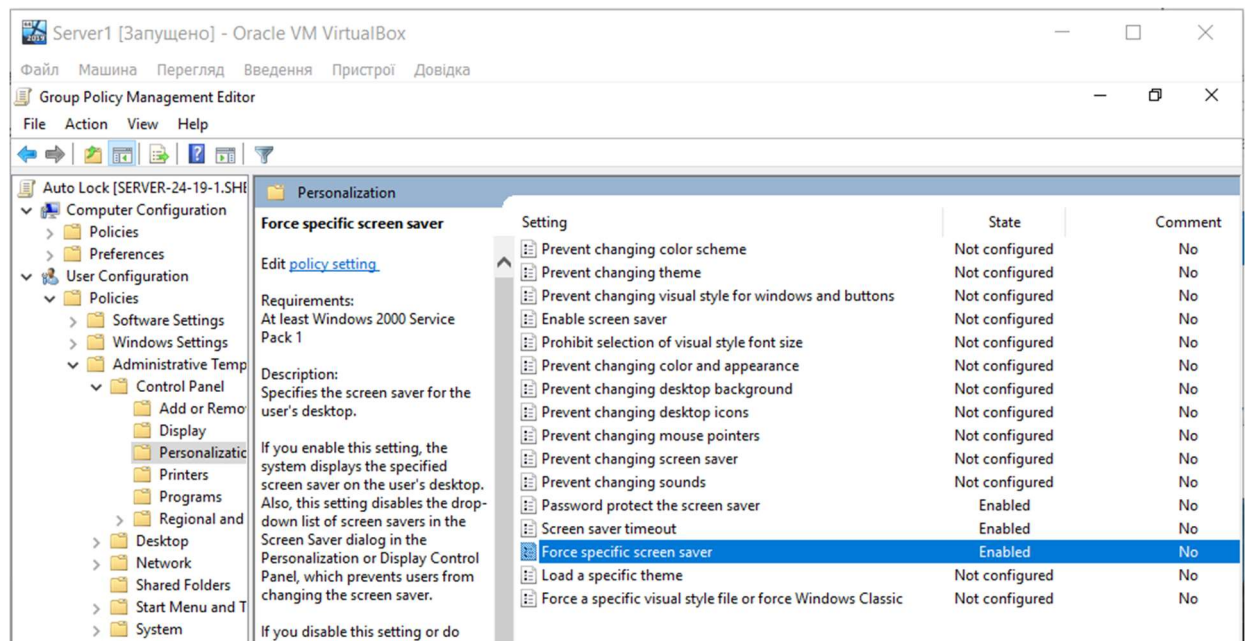


Рисунок 3.19 – Налаштування автоматичного блокування екрану

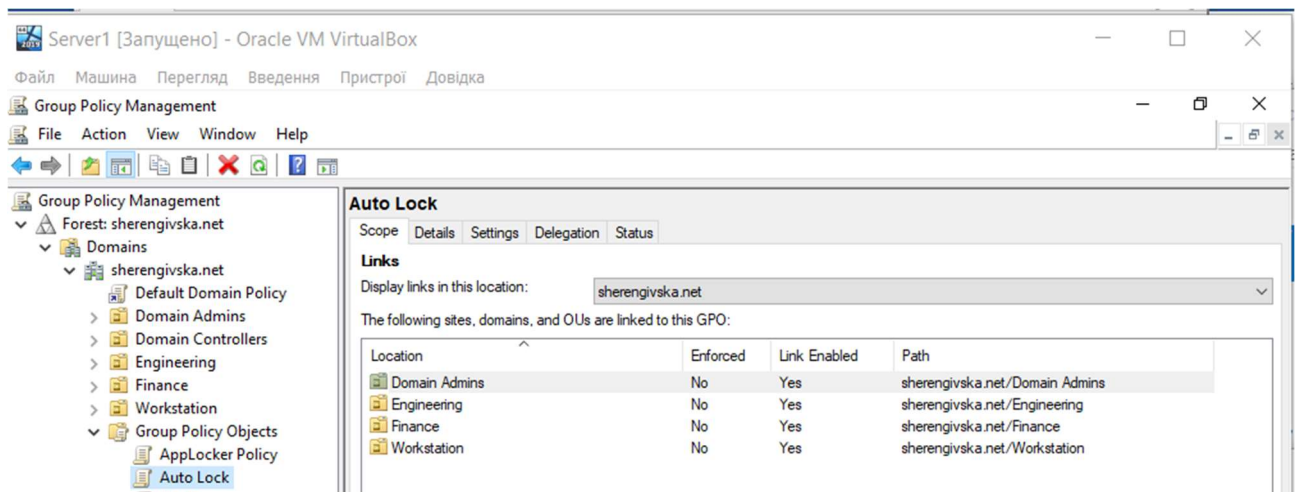


Рисунок 3.20 – Прив'язані OU до політики

Для адміністрування домену використовується одна привілейована робоча станція (РАW), налаштована згідно з рекомендаціями Microsoft. На ній не встановлено сторонніх додатків — зокрема, не використовуються веб-браузери, поштові клієнти, офісні пакети та інше програмне забезпечення, яке не пов'язане безпосередньо з адміністративними завданнями. Така ізоляція суттєво зменшує площину атак і підвищує захищеність облікових записів з підвищеними привілеями [15].

Створення РАW наведено на рисунках 3.21 – 3.24. Вхід дозволено лише обраним користувачам та заборона запуску програм. Це забезпечує безпечне середовище для виконання критичних адміністративних завдань.

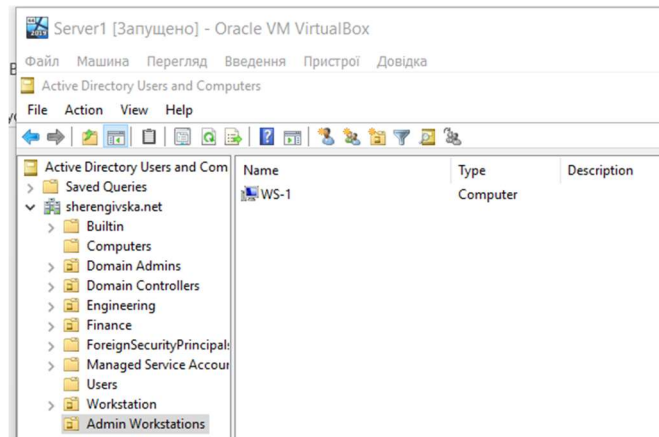


Рисунок 3.21 – Вибір привілейованої робочої станції

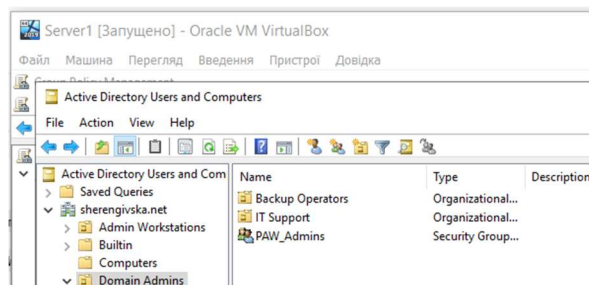


Рисунок 3.22 – Створена група адміністраторів

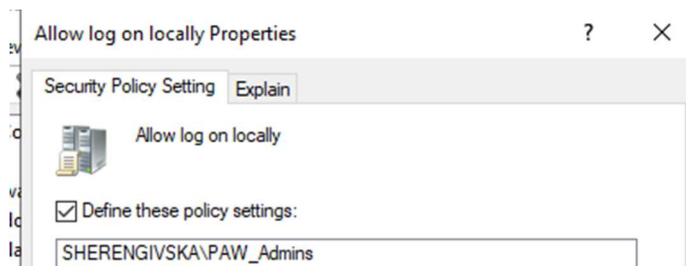


Рисунок 3.23 – Надання дозволу на вхід лише для привілейованої групи адміністраторів

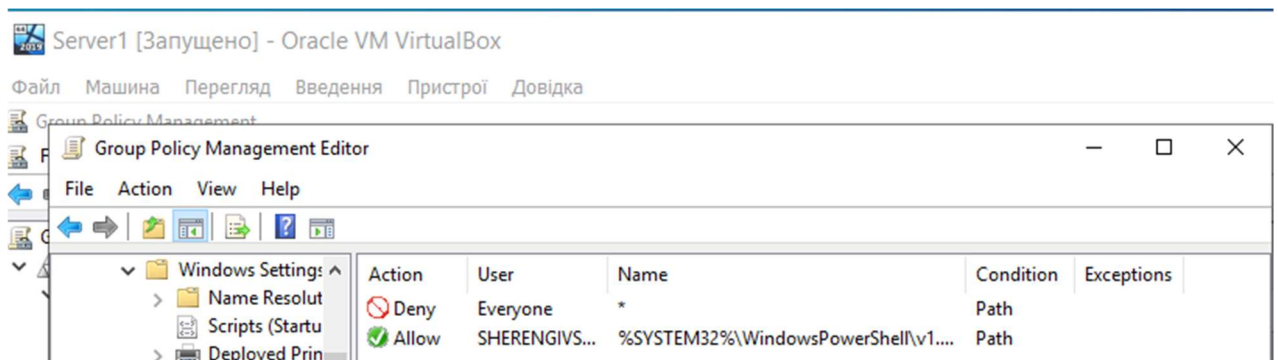


Рисунок 3.24 – Впровадження заборон запуску програм та дозволу запуску PowerShell

У доменній інфраструктурі було застосовано політику автоматичного оновлення для робочих станцій. Активовано параметр Configure Automatic

Updates, значення якого встановлено на 3 – Auto download and notify for install. Це дозволяє комп'ютерам, що входять до відповідної організаційної одиниці, автоматично завантажувати критичні оновлення без втручання адміністратора, сповіщаючи користувача про їхню готовність до встановлення. На рисунках 3.25 наведено налаштування політики, на рисунку 3.26 наведено на якій організаційній одиниці поширюється дана політика.

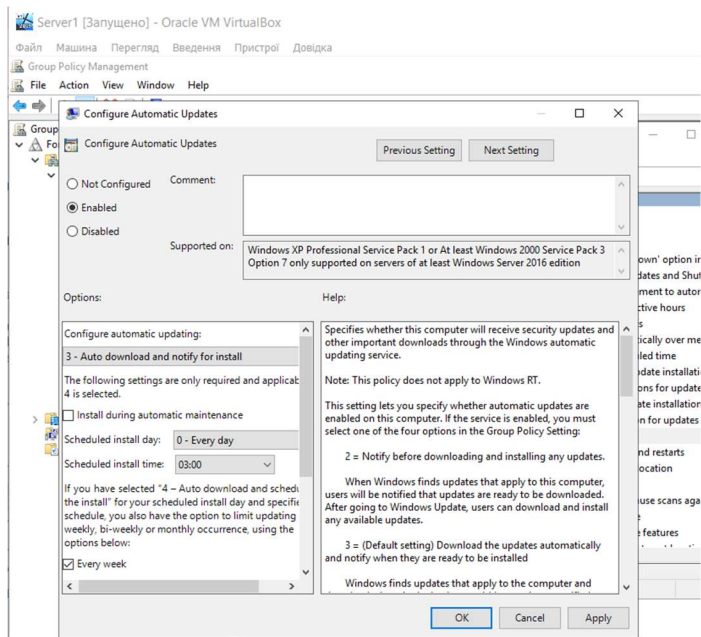


Рисунок 3.25 – Політика автоматичного оновлення системи

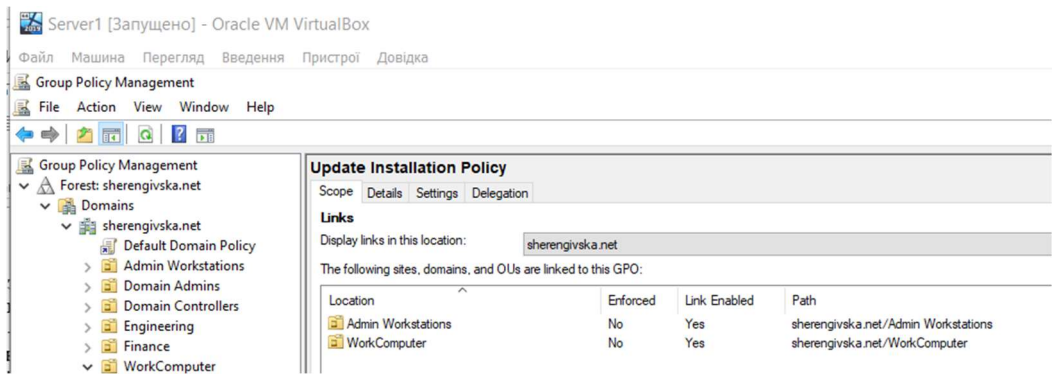


Рисунок 3.26 – Налаштування політики на організаційні одиниці

Саме завдяки правильно налаштованим політикам аудиту можна фіксувати дії користувачів, виявляти підозрілу активність та вчасно реагувати на потенційні загрози. Одним із ключових напрямів є моніторинг подій входу та виходу користувачів із системи, а також змін у файловій структурі.

На рисунку 3.27 наведено приклад налаштування політики аудиту для подій входу/виходу користувачів у домені, зокрема увімкнено аудит успішних та невдалих спроб авторизації.

На рисунку 3.28 показано налаштування аудиту файлової системи, що дозволяє реєструвати дії з файлами – наприклад, доступ, зміни чи спроби видалення.

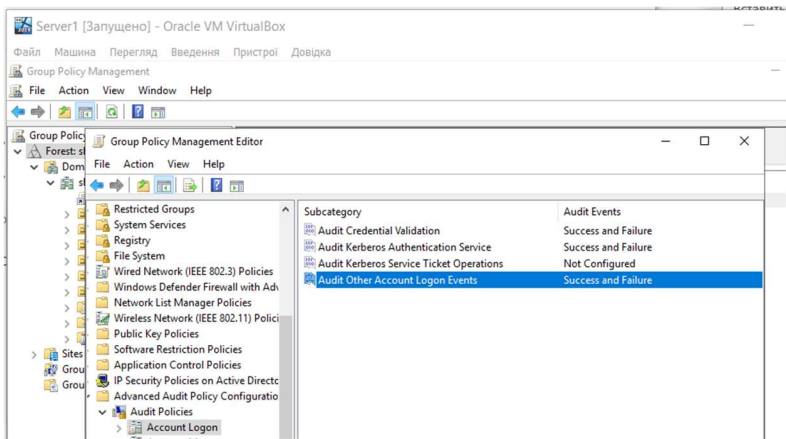


Рисунок 3.27 – Політика аудиту входу та виходу користувачів

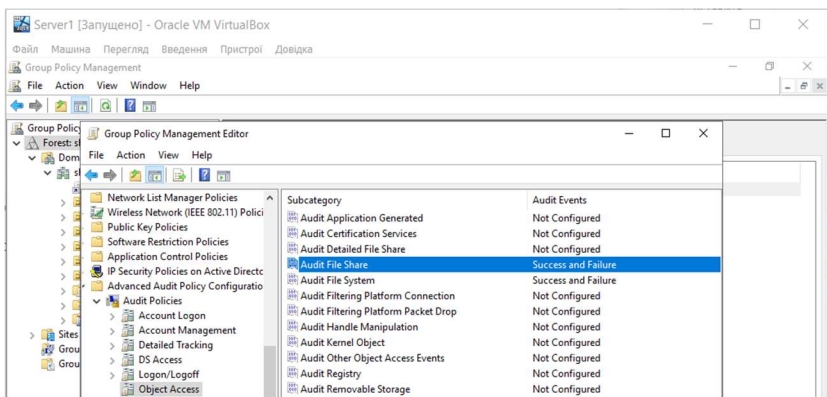


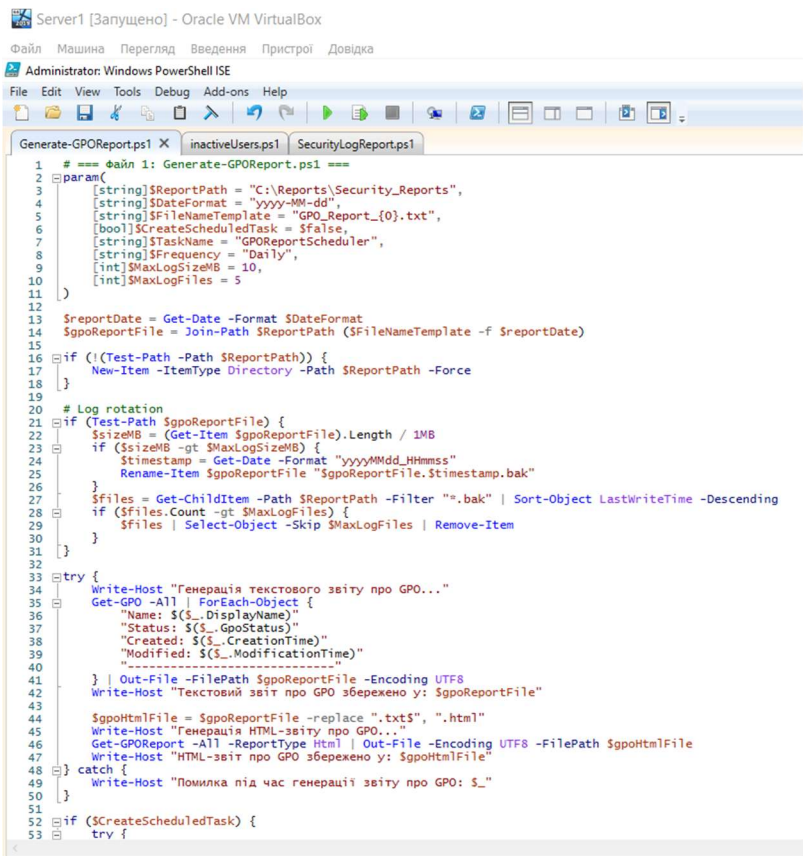
Рисунок 3.28 – Аудит доступу до файлів

Набір PowerShell-скриптів забезпечує зручне отримання звітів про GPO, неактивних користувачів і події безпеки. Вони легко читаються у текстовому форматі, налаштовуються під потреби та можуть запускатись за розкладом. Це спрощує моніторинг безпеки й економить час адміністратора.

На рисунку 3.29 зображено скрипт, який генерує звіт про наявні групові політики (GPO) у домені.

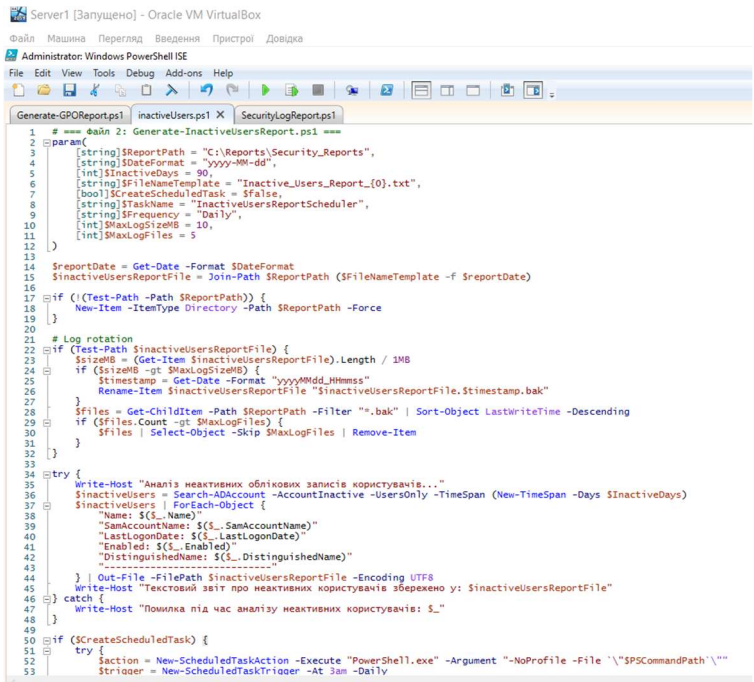
Рисунок 3.30 демонструє приклад скрипта, що виявляє неактивних користувачів, що може бути корисно для очищення домену та мінімізації потенційних ризиків.

А на рисунку 3.31 показано скрипт, який формує журнал логінів користувачів — один із важливих інструментів контролю автентифікаційної активності в системі.



```
1 # === Файл 1: Generate-GPOReport.ps1 ===
2 param(
3     [string]$ReportPath = "C:\Reports\Security_Reports",
4     [string]$DateFormat = "yyyy-MM-dd",
5     [string]$FileNameTemplate = "GPO_Report_{0}.txt",
6     [bool]$CreateScheduledTask = $false,
7     [string]$TaskName = "GPOReportScheduler",
8     [string]$Frequency = "Daily",
9     [int]$MaxLogSizeMB = 10,
10    [int]$MaxLogFiles = 5
11)
12
13 $ReportDate = Get-Date -Format $DateFormat
14 $GpoReportFile = Join-Path $ReportPath ($FileNameTemplate -f $ReportDate)
15
16 if (!(Test-Path -Path $ReportPath)) {
17     New-Item -ItemType Directory -Path $ReportPath -Force
18 }
19
20 # Log rotation
21 if (Test-Path $GpoReportFile) {
22     $SizeMB = (Get-Item $GpoReportFile).Length / 1MB
23     if ($SizeMB -gt $MaxLogSizeMB) {
24         $Timestamp = Get-Date -Format "yyyyMMdd_HHmmss"
25         Rename-Item $GpoReportFile "$GpoReportFile.$Timestamp.bak"
26     }
27     $Files = Get-Childitem -Path $ReportPath -Filter "*.bak" | Sort-Object LastWriteTime -Descending
28     if ($Files.Count -gt $MaxLogFiles) {
29         $Files | Select-Object -Skip $MaxLogFiles | Remove-Item
30     }
31 }
32
33 try {
34     Write-Host "Генерація текстового звіту про GPO..."
35     Get-GPO -All | ForEach-Object {
36         "Name: $($_.DisplayName)"
37         "Status: $($_.GpoStatus)"
38         "Created: $($_.CreationTime)"
39         "Modified: $($_.ModificationTime)"
40         "-----"
41     } | Out-File -FilePath $GpoReportFile -Encoding UTF8
42     Write-Host "Текстовий звіт про GPO збережено у: $GpoReportFile"
43
44     $GpoHtmlFile = $GpoReportFile -replace ".txt$", ".html"
45     Write-Host "Генерація HTML-звіту про GPO..."
46     Get-GPOReport -All -ReportType Html | Out-File -Encoding UTF8 -FilePath $GpoHtmlFile
47     Write-Host "HTML-звіт про GPO збережено у: $GpoHtmlFile"
48 } catch {
49     Write-Host "Помилка під час генерації звіту про GPO: $_"
50 }
51
52 if ($CreateScheduledTask) {
53     try {
54         $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-NoProfile -File \"\$SPSCmdPath\$ScriptName\""
```

Рисунок 3.29 – Скрипт, що виконує генерацію звіту про наявні GPO



```
1 # === Файл 2: Generate-InactiveUsersReport.ps1 ===
2 param(
3     [string]$ReportPath = "C:\Reports\Security_Reports",
4     [string]$DateFormat = "yyyy-MM-dd",
5     [int]$InactiveDays = 90,
6     [string]$FileNameTemplate = "Inactive_Users_Report_{0}.txt",
7     [bool]$CreateScheduledTask = $false,
8     [string]$TaskName = "InactiveUsersReportScheduler",
9     [string]$Frequency = "Daily",
10    [int]$MaxLogSizeMB = 10,
11    [int]$MaxLogFiles = 5
12)
13
14 $ReportDate = Get-Date -Format $DateFormat
15 $InactiveUsersReportFile = Join-Path $ReportPath ($FileNameTemplate -f $ReportDate)
16
17 if (!(Test-Path -Path $ReportPath)) {
18     New-Item -ItemType Directory -Path $ReportPath -Force
19 }
20
21 # Log rotation
22 if (Test-Path $InactiveUsersReportFile) {
23     $SizeMB = (Get-Item $InactiveUsersReportFile).Length / 1MB
24     if ($SizeMB -gt $MaxLogSizeMB) {
25         $Timestamp = Get-Date -Format "yyyyMMdd_HHmmss"
26         Rename-Item $InactiveUsersReportFile "$InactiveUsersReportFile.$Timestamp.bak"
27     }
28     $Files = Get-Childitem -Path $ReportPath -Filter "*.bak" | Sort-Object LastWriteTime -Descending
29     if ($Files.Count -gt $MaxLogFiles) {
30         $Files | Select-Object -Skip $MaxLogFiles | Remove-Item
31     }
32 }
33
34 try {
35     Write-Host "Аналіз неактивних облікових записів користувачів..."
36     $InactiveUsers = Search-AdAccount -AccountInactive -UsersOnly -TimeSpan (New-TimeSpan -Days $InactiveDays)
37     $InactiveUsers | ForEach-Object {
38         "Name: $($_.Name)"
39         "SamAccountName: $($_.SamAccountName)"
40         "LastLogonDate: $($_.LastLogonDate)"
41         "Enabled: $($_.Enabled)"
42         "DistinguishedName: $($_.DistinguishedName)"
43         "-----"
44     } | Out-File -FilePath $InactiveUsersReportFile -Encoding UTF8
45     Write-Host "Текстовий звіт про неактивних користувачів збережено у: $InactiveUsersReportFile"
46 } catch {
47     Write-Host "Помилка під час аналізу неактивних користувачів: $_"
48 }
49
50 if ($CreateScheduledTask) {
51     try {
52         $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument "-NoProfile -File \"\$SPSCmdPath\$ScriptName\""
```

Рисунок 3.30 – Скрипт, що виконує генерацію звіту про неактивних користувачів

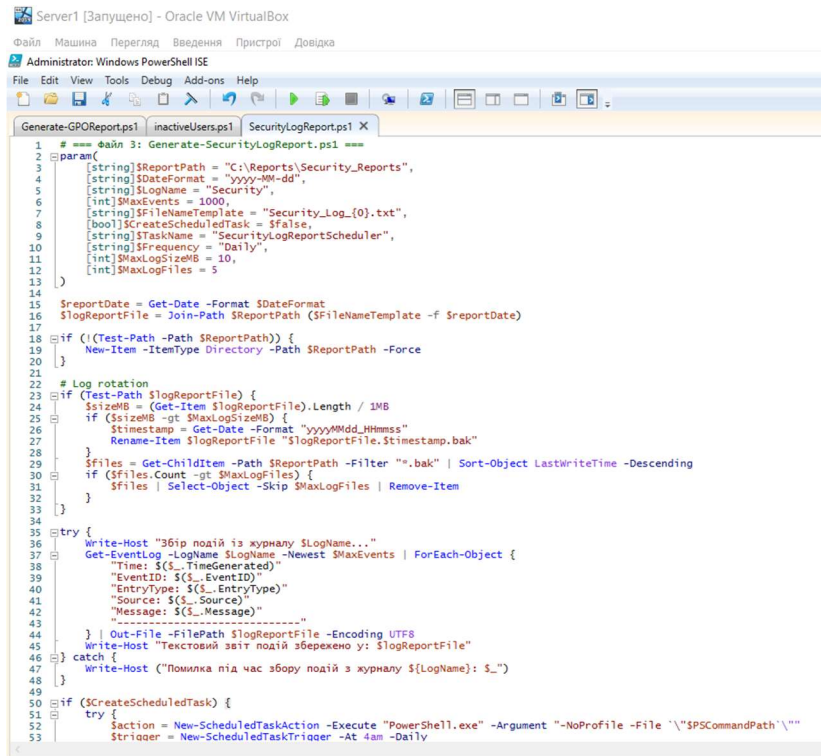


Рисунок 3.31 – Скрипт, що виконує генерацію звіту про залогінення

3.3 Перевірка роботи виконаних налаштувань.

Після всіх технічних налаштувань важливо переконаватися, що все працює так, як задумано. Наприклад, при першому вході користувача система просить змінити пароль – це захищає від ситуацій, коли тимчасовий пароль стає слабким місцем (див. рисунок 3.30).

Після оновлення пароля користувач успішно потрапляє до системи, що видно на рисунку 3.31 – усе працює плавно й без збоїв.

Окремо протестували й політику блокування: після п'яти невдалих спроб входу обліковий запис автоматично блокується. Це важливий захід проти підбору паролів, і як видно на рисунку 3.32, система спрацьовує чітко.

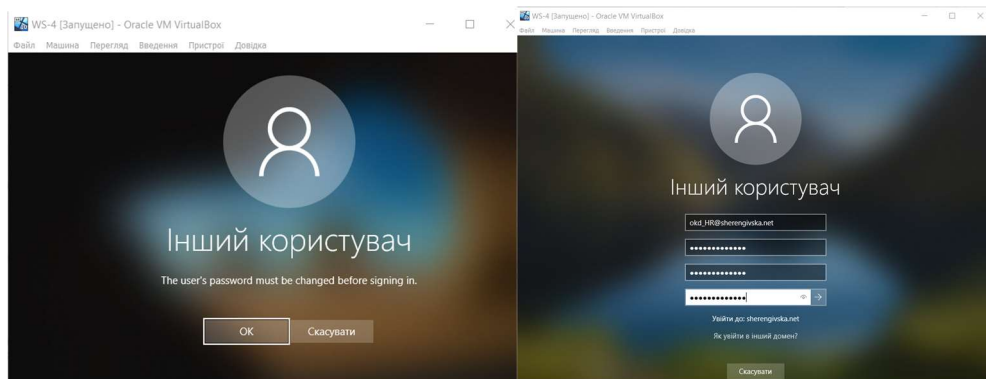


Рисунок 3.30 – Перший вхід під логіном і вимога замінити пароль

		Шеренгівська О.А.						Арк.
		Миколайчук В.В.						49
Змн.	Арк.	№ докум.	Підпис	Дата				

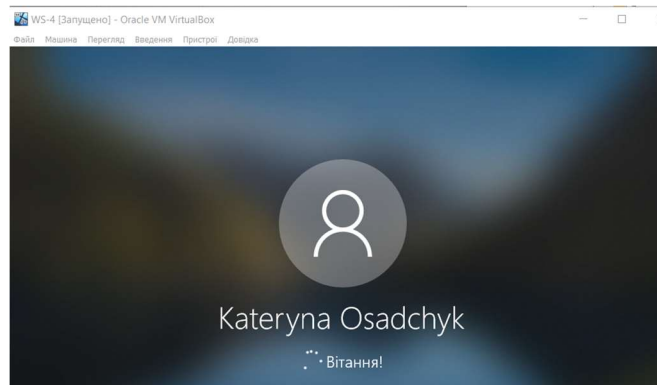


Рисунок 3.31 – Успішний вхід після зміни паролю

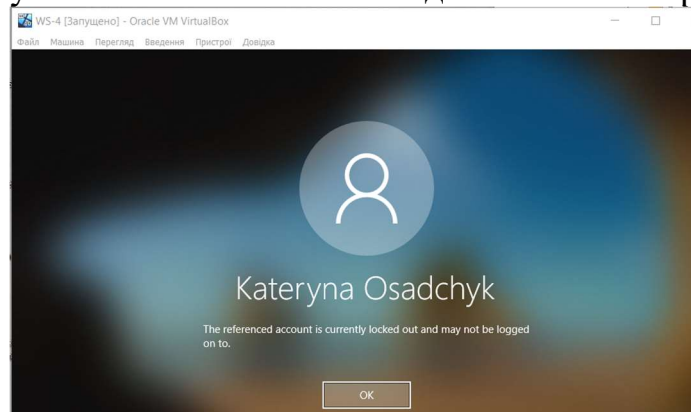


Рисунок 3.32 – Блокування акаунту після п'яти спроб невірної введення паролю

Ще одним важливим етапом стала перевірка механізму розблокування облікових записів. У випадку, коли обліковий запис користувача було заблоковано, його можна розблокувати лише з контролера домену – це забезпечує централізований контроль і унеможливорює самостійне зняття блокування користувачами (див. рисунок 3.33).

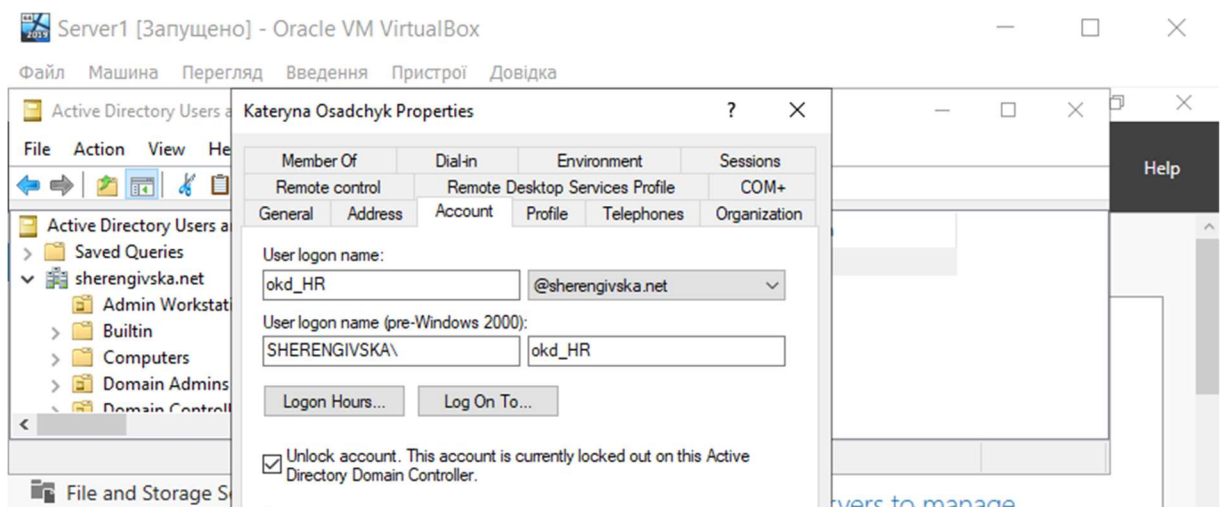


Рисунок 3.33 – Розблокування акаунту

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Після налаштування політики, що обмежує вхід лише з певної робочої станції, було проведено перевірку її роботи. Спочатку користувач Oleg Trado успішно виконав вхід на дозволений комп'ютер WS-9 – система впустила його без жодних зауважень (рисунк 3.34). Далі ми намагаємось увійти під цим самим обліковим записом з іншої машини, і все спрацювало як слід: система повідомила про заборону входу з цього пристрою (рисунк 3.35).



Рисунок 3.34 – Успішний вхід

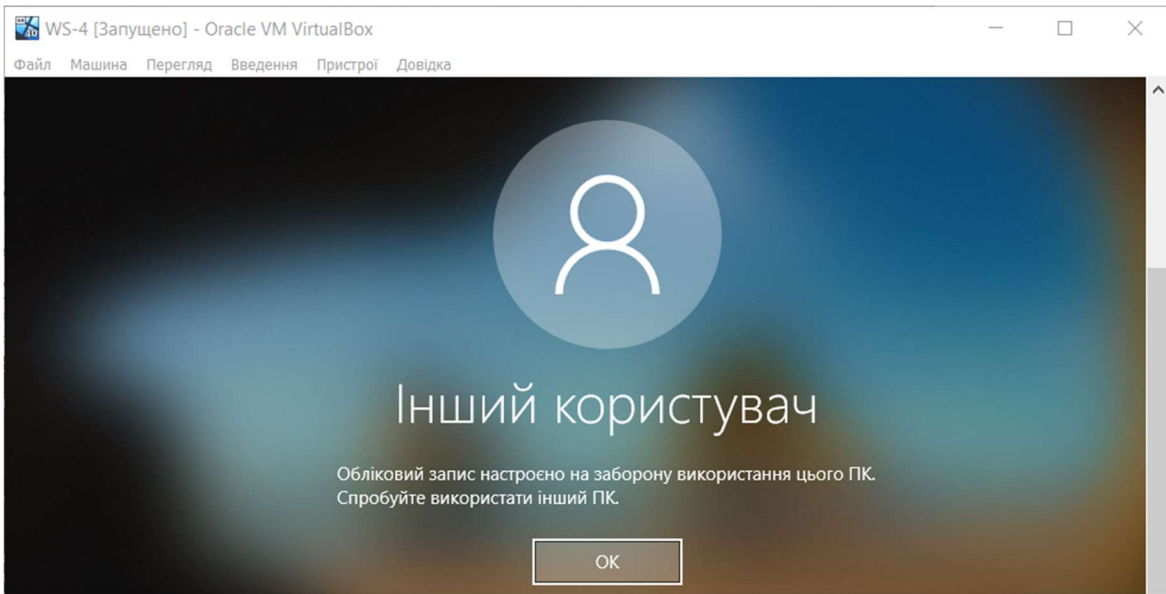


Рисунок 3.35 – Невдала спроба входу з іншої робочої станції

На рисунку 3.36 показано, як користувач намагається відкрити мережеву теку, доступ до якої йому заборонено. Система блокує спробу та повідомляє про відсутність прав. Це свідчить, що обмеження доступу працюють коректно.

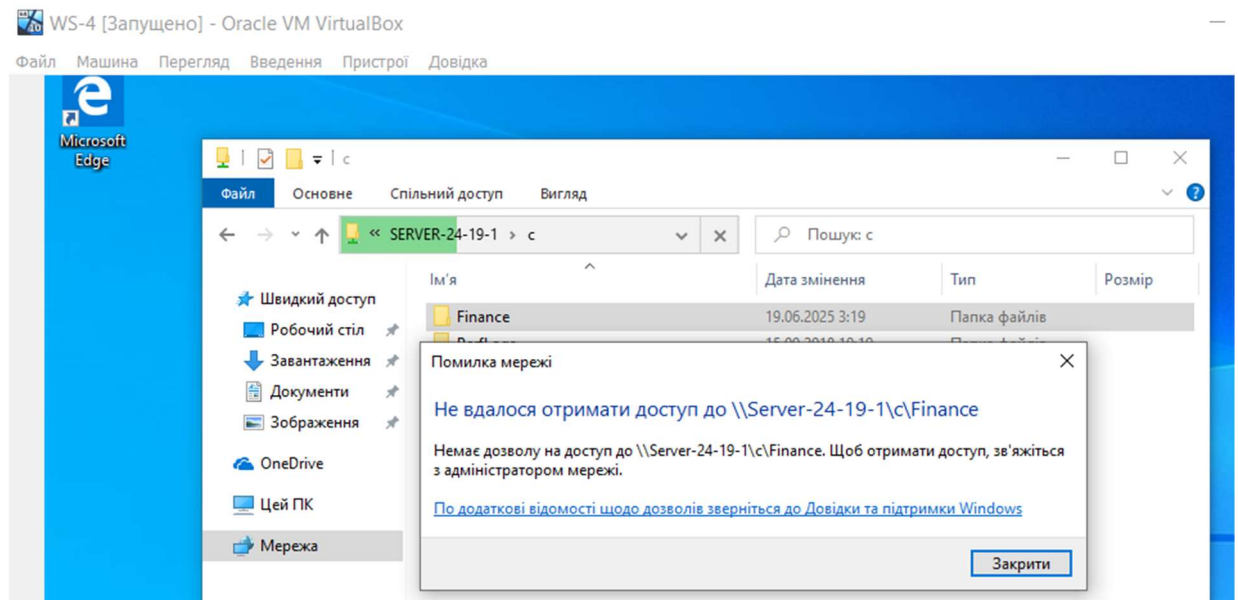


Рисунок 3.36 – Невдала спроба доступу до теки

У межах перевірка політика All Removable Storage classes: Deny all access було встановлено USB-накопичувач на клієнську машину. Система виявила пристрій, однак при спробі доступу отримано відмову, що наведено на рисунку 3.37.

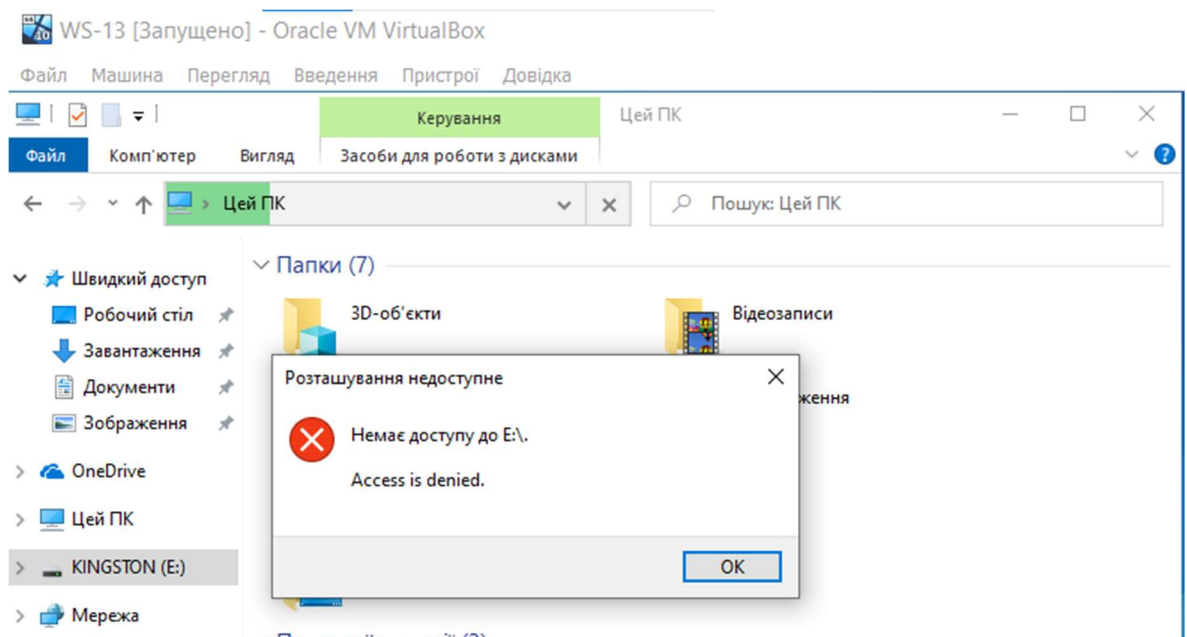


Рисунок 3.37 – Невдала спроба запуску флеш-носія

На рисунку 3.38 продемонстровано спробу запуску PowerShell, яка була заблокована політикою безпеки. З'являється повідомлення про обмеження, що підтверджує правильну дію встановлених правил доступу. Це допомагає знизити ризик виконання небезпечних команд.

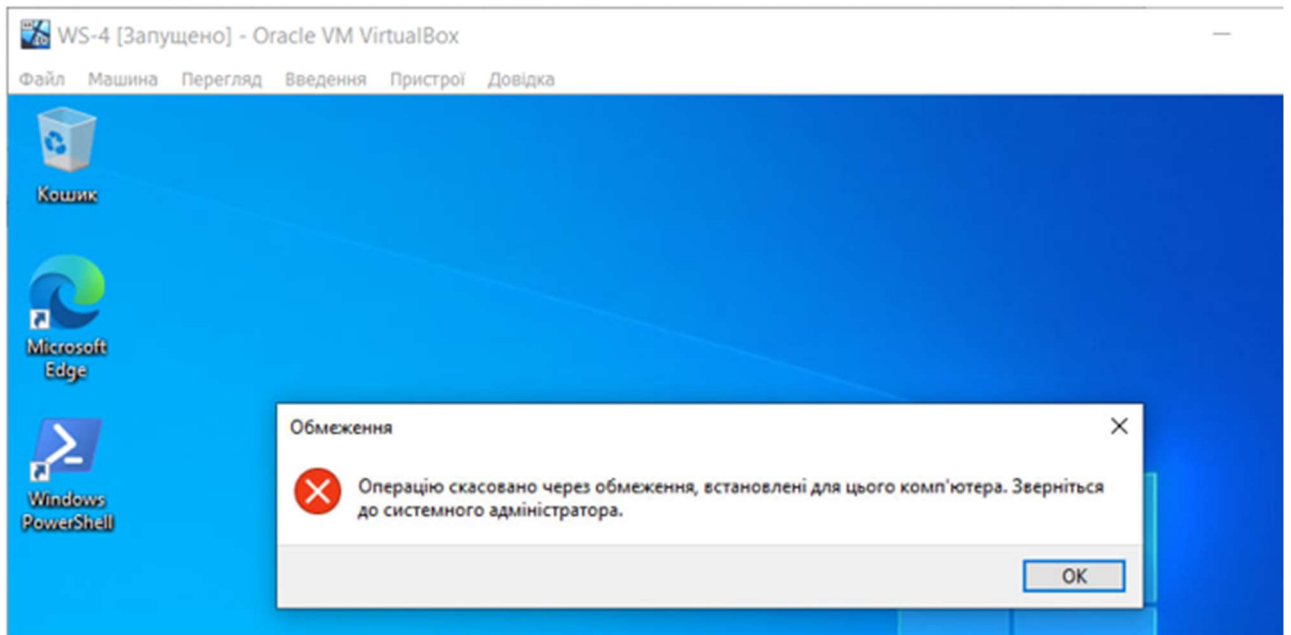


Рисунок 3.38 – Заборона відкриття PowerShell

Після налаштування RAW видно, що вхід дозволено лише адміністраторам мережі, інші користувачі отримують відмову (див. рисунок 3.39). Також заблоковано запуск сторонніх програм (див. рисунок 3.41). Це підтверджує, що політики безпеки працюють, як задумано.

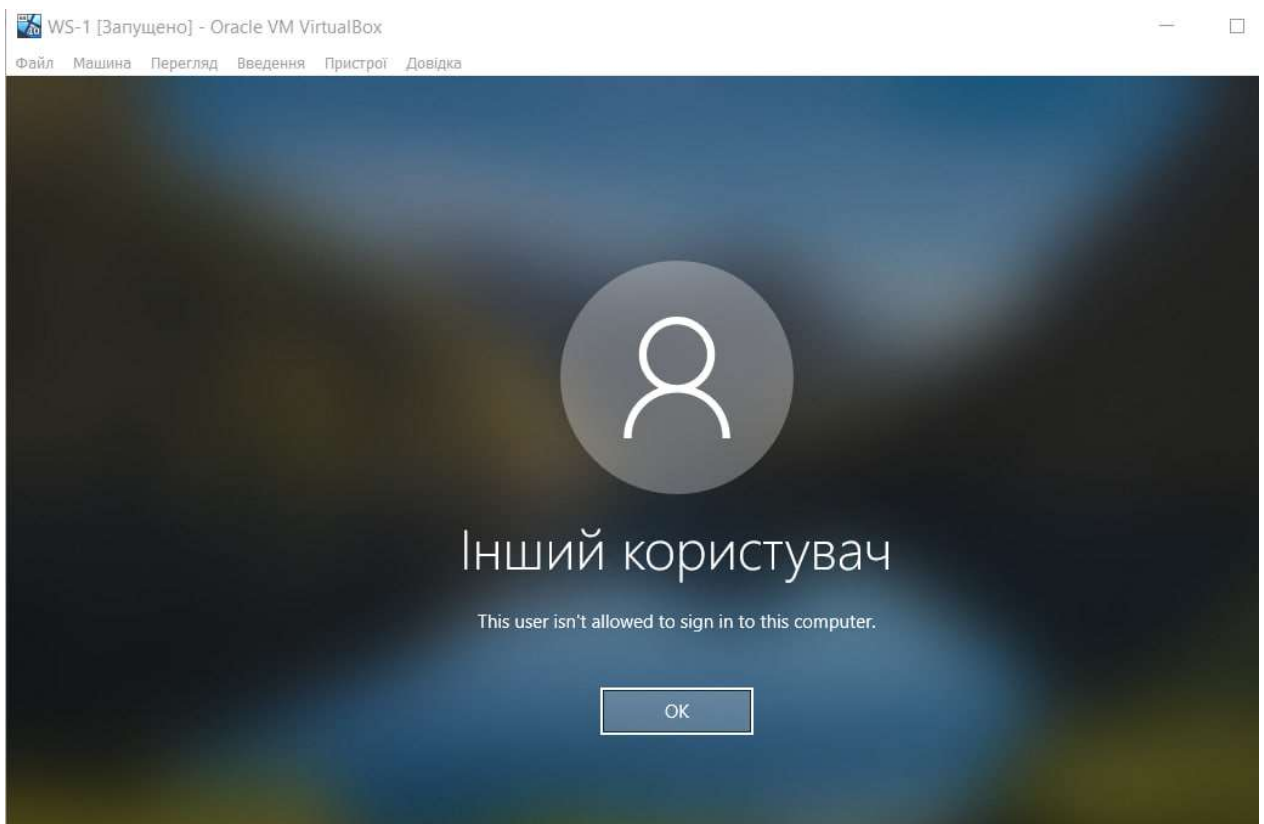


Рисунок 3.39 – Невдала спроба входу не під логіном адміністратора

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

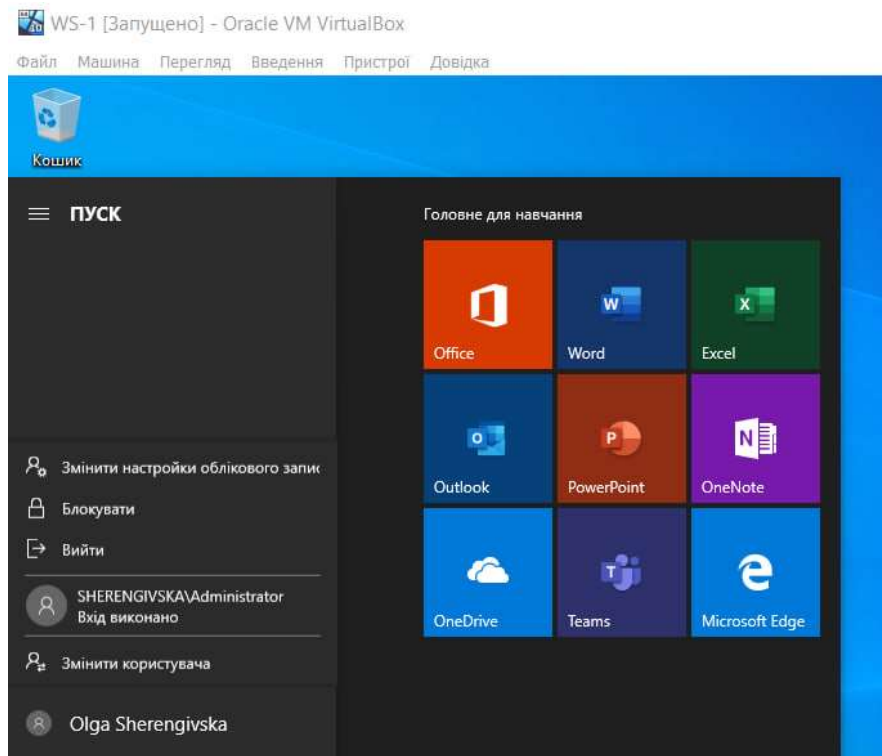


Рисунок 3.40 – Успішний вхід під логіном адміністратора

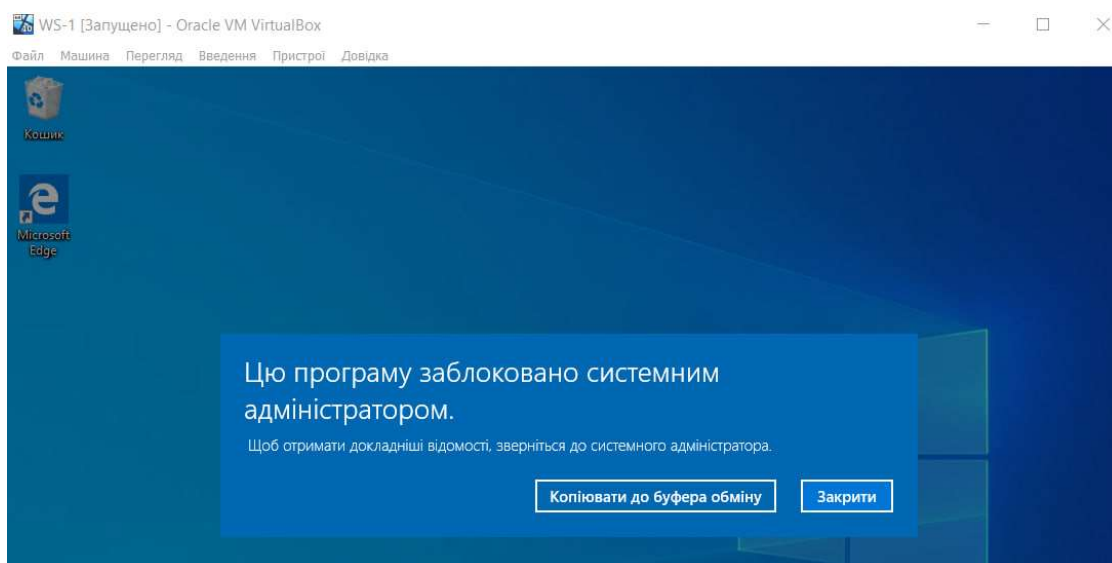


Рисунок 3.41 – Заборона запуску програм

На рисунках 3.42 – 3.43 показано результат застосування політики автоматичного оновлення до робочої станції в доменній інфраструктурі. У вікні параметрів Windows Update відображається повідомлення «Деякі налаштування встановлює ваша організація», що свідчить про активність групової політики, яка централізовано керує параметрами оновлення. У розділі з детальною інформацією про політики вказано, що параметри автоматичного оновлення, а також отримання оновлень для інших продуктів Microsoft були

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

задані адміністратором через групову політику. Це підтверджує, що політика була успішно застосована та діє на відповідний клієнтський комп’ютер.

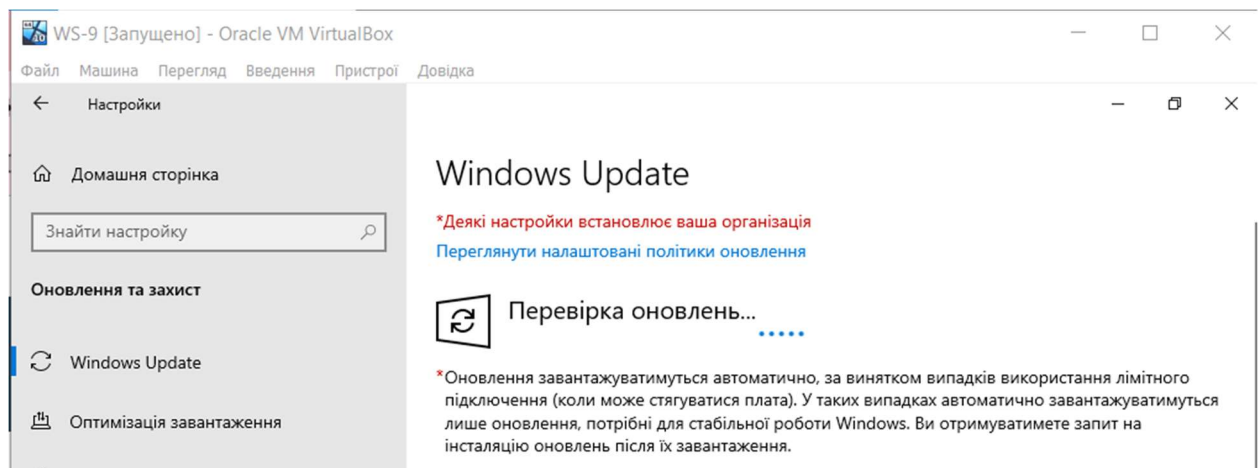


Рисунок 3.42 – Успішне керування оновленнями

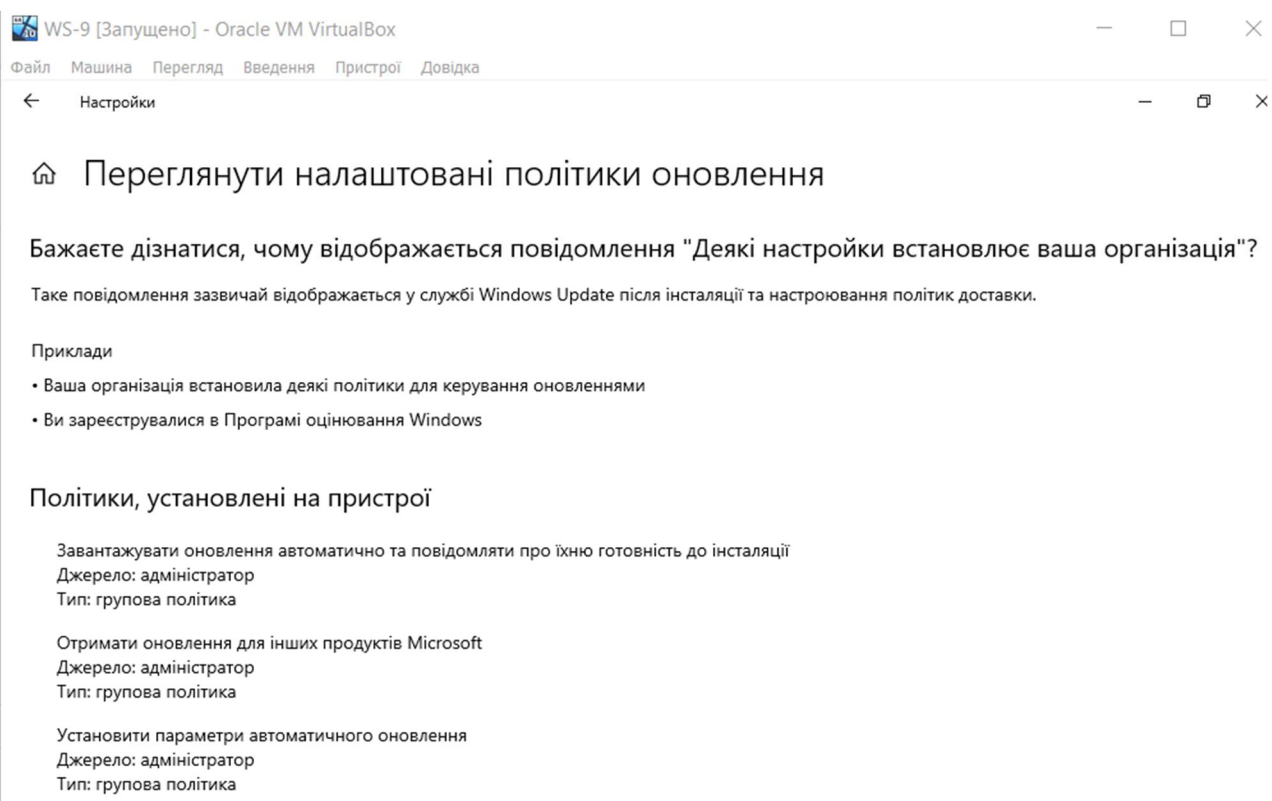


Рисунок 3.43 – Детальна інформація щодо встановленої політики

На рисунку 3.44 представлено журнал подій, у якому видно всі ключові дії, пов’язані з безпекою: автентифікація користувачів, доступ до спільних ресурсів, а також використання служби Kerberos.

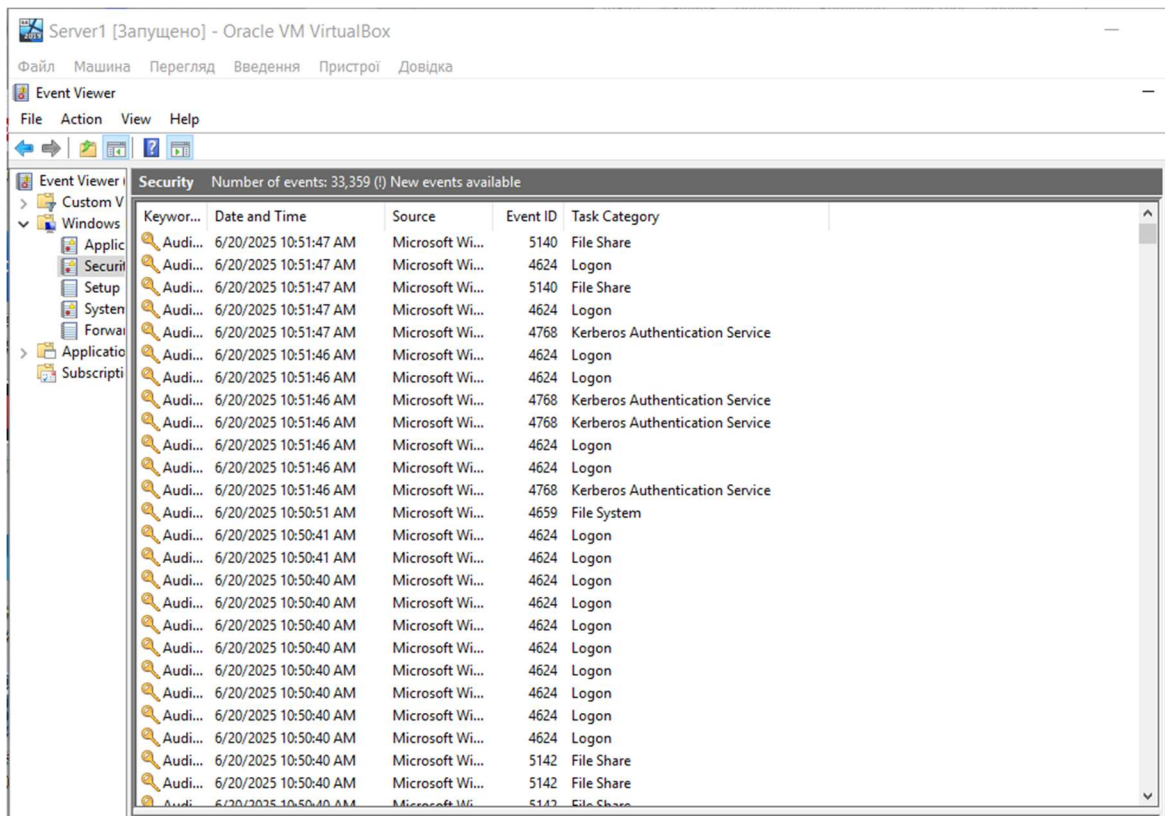


Рисунок 3.44 – Перегляд аутентифікації користувачів, зміни у групах безпеки, доступ до ресурсів

На рисунку 3.45 показано результати роботи скрипта, який відображає застосовані політики безпеки.

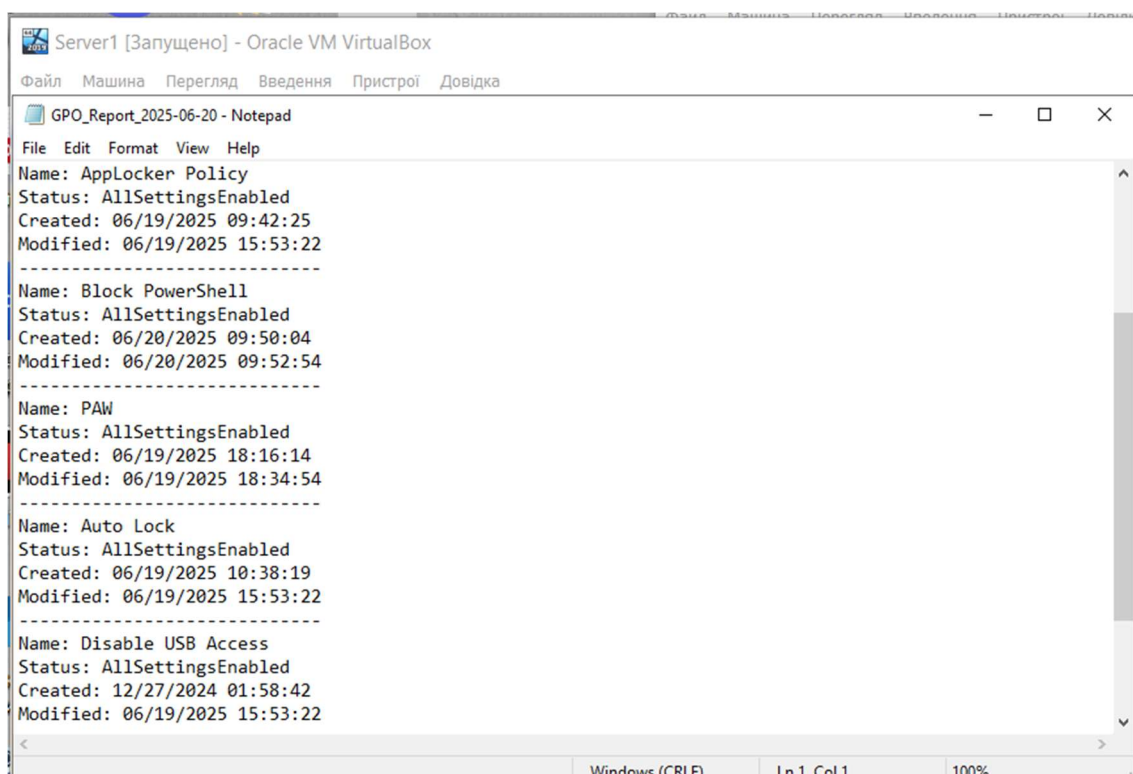


Рисунок 3.45 – Політики GPO

Рисунок 3.46 демонструє список неактивних користувачів, що допомагає вчасно виявляти облікові записи без активності.

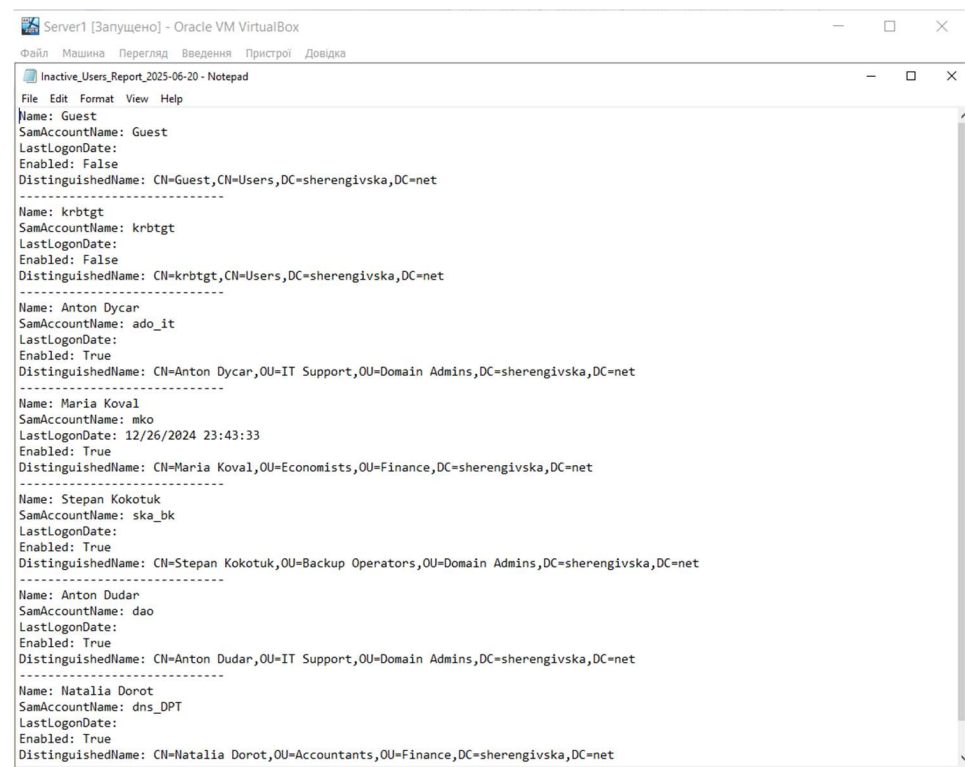


Рисунок 3.46 – Неактивні користувачі
На рисунку 3.47 видно деталізований запис події входу в систему — це дає змогу контролювати активність користувачів та перевіряти права доступу.

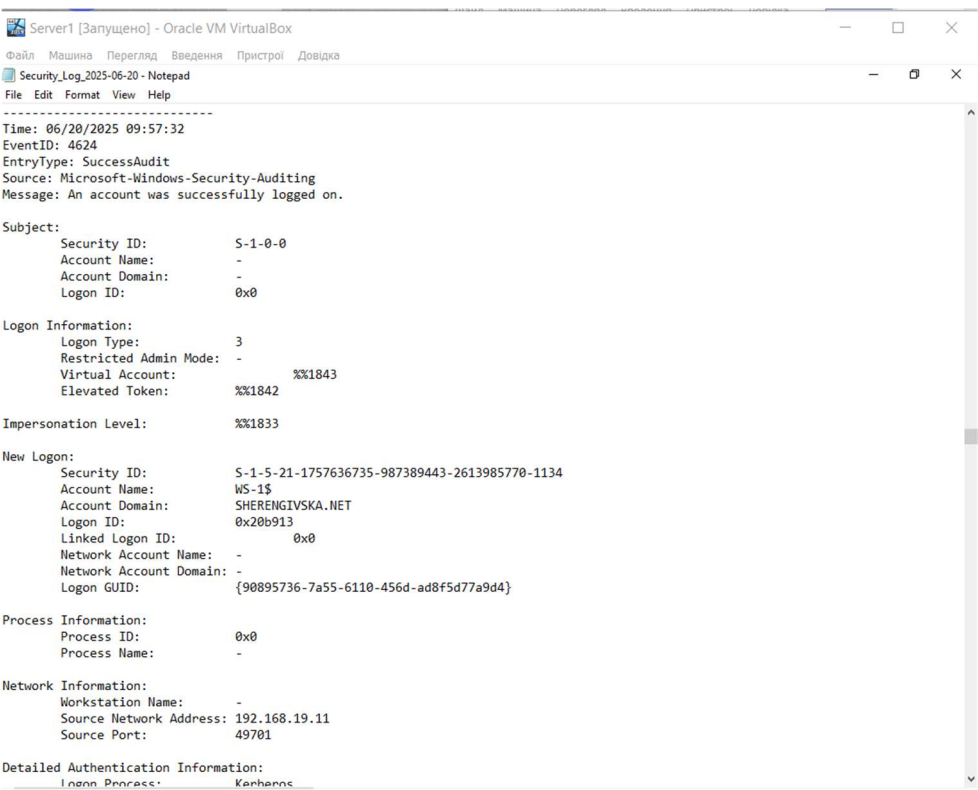


Рисунок 3.47 – Інформація про залогування (скріншот обрізаний)

Висновок до третього розділу

У цьому розділі було здійснено практичну реалізацію заходів із захисту корпоративної мережі на базі Active Directory. В ході роботи створено доменне середовище, налаштовано контролери домену, реалізовано базові політики безпеки, а також обмежено права доступу до критично важливих ресурсів. Було впроваджено політики блокування облікових записів, паролльні вимоги згідно з рекомендаціями безпекових стандартів, налаштовано аудит ключових подій, обмежено запуск небезпечних інструментів на робочих станціях через AppLocker.

Також протестовано практичне застосування політик: виконано перевірку входу користувачів, блокування при багаторазовому введенні неправильного пароля, недопуск до заборонених ПК, заборона відкриття певних програм і доступу до мережових тек. Реалізовано другий контролер домену для підвищення стійкості до збоїв та забезпечення надійності реплікації даних.

Використання PowerShell-скриптів дало змогу автоматизувати моніторинг безпеки та зібрати звіти щодо політик, активності користувачів і подій входу. Усі налаштування були протестовані, що підтверджено відповідними скріншотами, наведеними в підрозділі перевірки.

Таким чином, розділ демонструє, як за допомогою вбудованих інструментів Windows Server, групових політик і засобів моніторингу можна ефективно захистити корпоративну мережу на основі Active Directory, дотримуючись сучасних вимог інформаційної безпеки.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи вдалося досягти поставленої мети — спроектувати й реалізувати підсистему захисту корпоративної мережі з використанням служби Active Directory. Робота охопила як теоретичний аналіз сучасних підходів до безпеки, так і практичну реалізацію на основі обґрунтованого вибору архітектури та технологій.

На початковому етапі було досліджено роль AD у корпоративних середовищах, зокрема її важливість як інструменту централізованого управління доступом, обліковими записами та політиками безпеки. Аналіз поширених векторів атак і вразливостей дозволив сформулювати чітке розуміння того, чому неналежна конфігурація AD може призвести до серйозних наслідків для всієї організації.

У процесі роботи було побудовано мережеву інфраструктуру із використанням VLAN-сегментування та протоколу HSRP для резервування шлюзів. Це дозволило забезпечити логічне розмежування доступу, підвищити гнучкість управління й гарантувати відмовостійкість мережі. Окрему увагу приділено реалізації групових політик (GPO), зокрема блокуванню доступу до небезпечних інструментів, таких як PowerShell, обмеженню використання зовнішніх носіїв, жорстким вимогам до паролів і політиці блокування облікових записів. Додатково було впроваджено моніторинг за допомогою PowerShell-скриптів, що дозволило централізовано збирати звіти про стан системи, активність користувачів і спроби входу до системи. Це сприяло як своєчасному виявленню підозрілої активності, так і зручному аудиту подій безпеки.

Під час реалізації враховано сучасні вимоги до інформаційної безпеки та застосовано ключові принципи захисту, включаючи мінімізацію привілеїв, централізований аудит, обмеження прав доступу та сегментацію мережі. Для підвищення надійності інфраструктури було впроваджено другий контролер домену.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Зважаючи на перспективу подальшого розвитку, доцільним є розширення впроваджених засобів безпеки через інтеграцію додаткових протоколів і технологій. Зокрема, йдеться про IPsec для шифрування трафіку, DNSSEC для захисту від підміни записів DNS, SMB Signing для перевірки цілісності даних у процесі передачі, а також LAPS для безпечного управління локальними паролями. Упровадження системи умовного доступу та інтеграція з SIEM-рішеннями можуть суттєво підвищити рівень оперативного реагування на загрози. Крім того, застосування практик, описаних у фреймворках NIST SP 800-53 або CIS Controls, дозволить забезпечити високий рівень відповідності сучасним вимогам інформаційної безпеки та регуляторним стандартам.

Таким чином, у межах дипломної роботи було створено стабільну, масштабовану й безпечну модель корпоративної мережі, яка відповідає сучасним стандартам захисту та є придатною для подальшого розвитку. Реалізовані заходи, зокрема впровадження VLAN, HSRP, SSH, STP, політик групової безпеки, моніторинг дій користувачів та контроль доступу, довели свою ефективність у тестовому середовищі. Запропоновану архітектуру можна адаптувати для практичного впровадження в організаціях різного масштабу — від невеликих офісів до великих підприємств з підвищеними вимогами до безпеки критичних сервісів.

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Active Directory Domain Services overview [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
2. These Are Some Major Active Directory Threats Lurking in Your Network. [Електронний ресурс] – Режим доступу: <https://fidelissecurity.com/threatgeek/active-directory-security/major-active-directory-threats/>
3. Best practices for securing Active Directory [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>
4. Getting Started with GNS3 [Електронний ресурс] – Режим доступу: <https://docs.gns3.com/docs/>
5. Cisco Systems. ISR 4000 Series Integrated Services Routers. [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/site/us/en/products/networking/sdwan-routers/4000-series-integrated-services-routers/index.html>
6. CISCO CATALYST 3560 Series Switches Hardware View [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/3560.html>
7. Cisco Catalyst 2960-S and 2960 Series Switches with LAN Lite Software Data Sheet [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd806b0bd8.html
8. Windows 10 editions for education customers [Електронний ресурс] – Режим доступу: <https://support.microsoft.com/en-us/topic/windows-10-editions-for-education-customers-bf2572aa-5555-2b1e-f7ce-81e8ba890444>

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Hardware requirements for Windows Server. [Електронний ресурс] Режим доступу: <https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements?tabs=cpu&pivots=windows-server-2025>

10. Найкращі інструменти управління груповими політиками [Електронний ресурс]. – Режим доступу: <https://corewin.ua/blog/top-group-policy-management-tools/>

11. Automating Active Directory Management with PowerShell [Електронний ресурс]. – Режим доступу: <https://tomtalksit.itsupportpro.uk/automating-active-directory-management-with-powershell-09e728834582>

12. NIST. Security and Privacy Controls for Information Systems and Organizations: NIST SP 800-53 Rev. 5 [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

13. ISO/IEC 27002:2022 – Control 5.17 – Authentication information. [Електронний ресурс]. – Режим доступу: https://www.isms.online/iso-27002/control-5-17-authentication-information/?utm_source

14. Kerberos Policy [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/kerberos-policy>

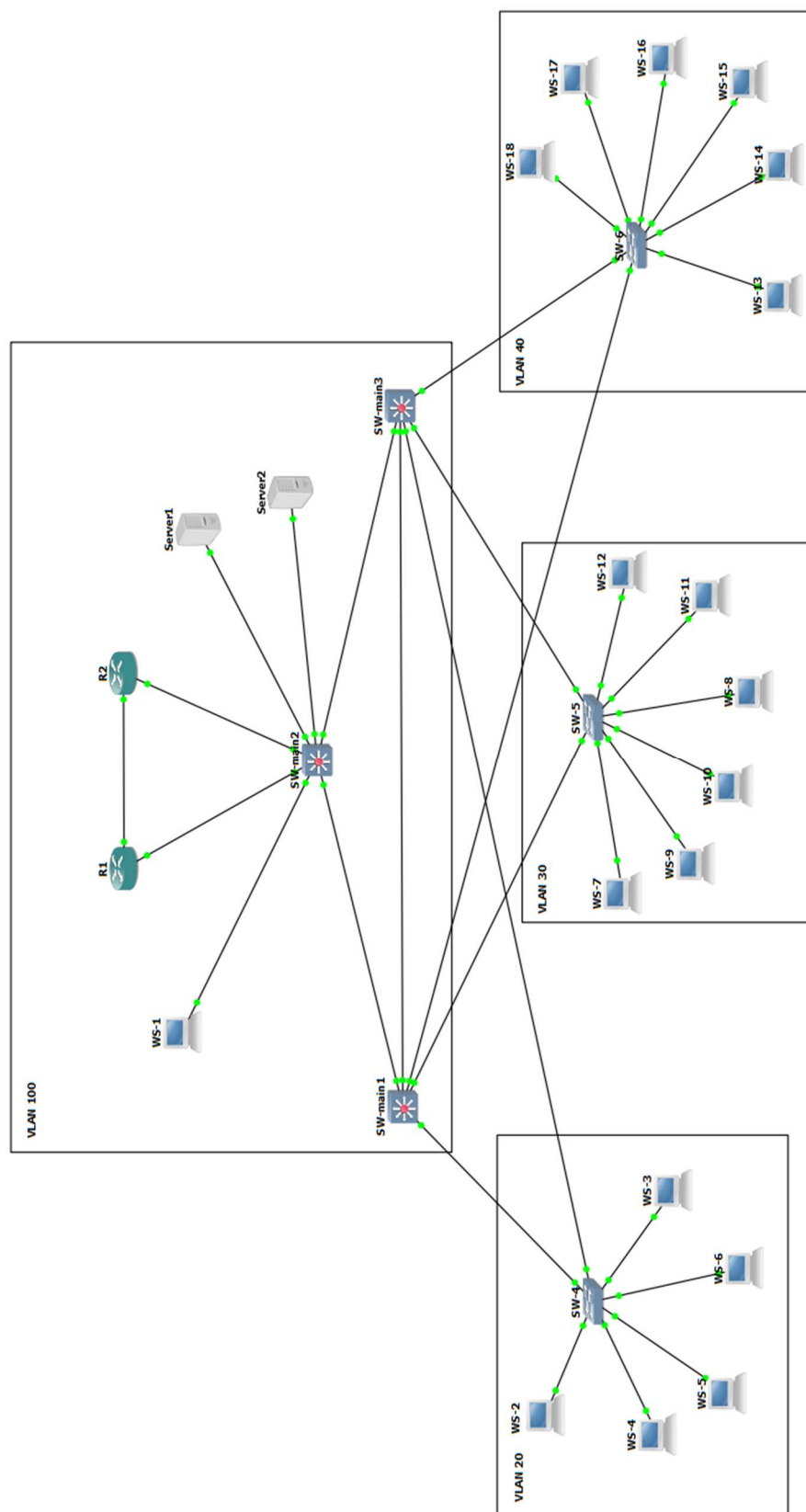
15. Microsoft. Privileged Access Workstations – Learn Microsoft [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/security/privileged-access-workstations/legacy-privileged-access-devices>

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				63
Змн.	Арк.	№ докум.	Підпис	Дата		

Побудована мережа



		Шеренгівська О.А.		
		Миколайчук В.В.		
Змн.	Арк.	№ докум.	Підпис	Дата

ККІКБ.КР.Б – 125 – 19 – ПЗ

Арк.

64

Конфігураційні файли пристроїв

R1

R1#sh run	no ip domain lookup
Building configuration...	ip domain name corp.local
	ip cef
Current configuration : 3113 bytes	no ipv6 cef
!	!
! Last configuration change at	multilink bundle-name authenticated
12:02:53 UTC Fri Jun 20 2025	!
upgrade fpd auto	username admin privilege 15 secret 5
version 15.2	\$1\$B1b5\$Hc.RK1p8EKmIjSK0G3JK
service timestamps debug datetime	H1
msec	!
service timestamps log datetime msec	redundancy
no service password-encryption	!
!	!
hostname R1	ip tcp synwait-time 5
!	ip ssh time-out 60
boot-start-marker	ip ssh version 2
boot-end-marker	!
!	interface FastEthernet0/0
!	description Link to R2
!	ip address 192.168.255.1
no aaa new-model	255.255.255.252
no ip icmp rate-limit unreachable	duplex half
!	!
!	interface FastEthernet1/0
!	no ip address

```

shutdown
duplex auto
speed auto
!
interface FastEthernet1/0.20
description VLAN 20 - Workstations
encapsulation dot1Q 20
ip address 192.168.20.1
255.255.255.0
standby 20 ip 192.168.20.10
standby 20 priority 110
standby 20 preempt
!
interface FastEthernet1/0.30
description VLAN 30 - Engineering
encapsulation dot1Q 30
ip address 192.168.30.1
255.255.255.0
standby 30 ip 192.168.30.10
standby 30 priority 110
standby 30 preempt
!
interface FastEthernet1/0.40
description VLAN 40 - Finance
encapsulation dot1Q 40
ip address 192.168.40.1
255.255.255.0
standby 40 ip 192.168.40.10
standby 40 priority 110
standby 40 preempt
!
interface FastEthernet1/0.100
description VLAN 100 - Management
encapsulation dot1Q 100
ip address 192.168.19.1
255.255.255.240
standby 100 ip 192.168.19.3
standby 100 priority 110
standby 100 preempt
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial2/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/2
no ip address
shutdown

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

serial restart-delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
!
interface GigabitEthernet3/0
no ip address
shutdown
negotiation auto
!
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 auto
speed auto
!
interface FastEthernet5/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial6/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial6/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial6/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial6/3
no ip address
shutdown
serial restart-delay 0
!
ip forward-protocol nd
no ip http server

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no ip http secure-server
!
!
!
ip access-list standard SSH_ONLY
permit 192.168.19.0 0.0.0.15
!
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
access-class SSH_ONLY in
login local
transport input ssh
!
!
end

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

R2	!
R2#sh run	!
Building configuration...	no ip domain lookup
	ip domain name corp.local
Current configuration : 3119	ip cef
bytes	no ipv6 cef
!	!
! Last configuration change at	multilink bundle-name
12:06:53 UTC Fri Jun 20 2025	authenticated
upgrade fpd auto	!
version 15.2	username admin privilege 15
service timestamps debug	secret 5
datetime msec	\$1\$7K65\$xNKKt4.PTYnvWpXre4oX
service timestamps log datetime	V0
msec	!
no service password-encryption	redundancy
!	!
hostname R2	!
!	ip tcp synwait-time 5
boot-start-marker	ip ssh time-out 60
boot-end-marker	ip ssh version 2
!	!
!	!
!	interface FastEthernet0/0
no aaa new-model	description Link to R1
no ip icmp rate-limit unreachable	ip address 192.168.255.2
!	255.255.255.252
!	duplex half
!	!
!	interface FastEthernet1/0

```

no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0.20
  description VLAN 20 -
  Workstations
  encapsulation dot1Q 20
  ip address 192.168.20.2
  255.255.255.0
  standby 20 ip 192.168.20.10
  standby 20 priority 90
  standby 20 preempt
!
interface FastEthernet1/0.30
  description VLAN 30 -
  Engineering
  encapsulation dot1Q 30
  ip address 192.168.30.2
  255.255.255.0
  standby 30 ip 192.168.30.10
  standby 30 priority 90
  standby 30 preempt
!
interface FastEthernet1/0.40
  description VLAN 40 - Finance
  encapsulation dot1Q 40
  ip address 192.168.40.2
  255.255.255.0

```

```

standby 40 ip 192.168.40.10
standby 40 priority 90
standby 40 preempt
!
interface FastEthernet1/0.100
  description VLAN 100 -
  Management
  encapsulation dot1Q 100
  ip address 192.168.19.2
  255.255.255.240
  standby 100 ip 192.168.19.3
  standby 100 priority 90
  standby 100 preempt
!
interface FastEthernet1/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial2/0
  no ip address
  shutdown
  serial restart-delay 0
!
interface Serial2/1
  no ip address
  shutdown
  serial restart-delay 0
!

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

interface Serial2/2	shutdown
no ip address	duplex auto
shutdown	speed auto
serial restart-delay 0	!
!	interface FastEthernet5/1
interface Serial2/3	no ip address
no ip address	shutdown
shutdown	duplex auto
serial restart-delay 0	speed auto
!	!
interface GigabitEthernet3/0	interface Serial6/0
no ip address	no ip address
shutdown	shutdown
negotiation auto	serial restart-delay 0
!	!
interface FastEthernet4/0	interface Serial6/1
no ip address	no ip address
shutdown	shutdown
duplex auto	serial restart-delay 0
speed auto	!
!	interface Serial6/2
interface FastEthernet4/1	no ip address
no ip address	shutdown
shutdown	serial restart-delay 0
duplex auto	!
speed auto	interface Serial6/3
!	no ip address
interface FastEthernet5/0	shutdown
no ip address	serial restart-delay 0

```

!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
ip access-list standard
SSH_ONLY
    permit 192.168.19.0 0.0.0.15
!
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
    access-class SSH_ONLY in
    login local
    transport input ssh
!
!
End

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-main2#sh run	!
Building configuration...	ip cef
	!
Current configuration : 2517 bytes	!
!	no ip domain-lookup
! Last configuration change at	no ipv6 cef
14:51:07 UTC Wed Jun 25 2025	ipv6 multicast rpf use-bgp
!	!
version 15.1	!
service timestamps debug datetime	!
msec	!
service timestamps log datetime msec	!
no service password-encryption	!
service compress-config	!
!	!
hostname SW-main2	!
!	spanning-tree mode rapid-pvst
boot-start-marker	spanning-tree extend system-id
boot-end-marker	!
!	vlan internal allocation policy
!	ascending
	!
logging discriminator EXCESS	ip tcp synwait-time 5
severity drops 6 msg-body drops	!
EXCESSCOLL	!
logging buffered 50000	
logging console discriminator	interface Ethernet0/0
EXCESS	description Server1 link
!	switchport access vlan 100
no aaa new-model	switchport mode access
no ip icmp rate-limit unreachable	duplex auto

```

spanning-tree portfast
!
interface Ethernet0/1
    duplex auto
!
interface Ethernet0/2
    description Link to Server2
    switchport access vlan 100
    switchport mode access
    duplex auto
!
interface Ethernet0/3
    duplex auto
!
interface Ethernet1/0
    description Admin PC - WS-1
    switchport access vlan 100
    switchport mode access
    duplex auto
    spanning-tree portfast
!
interface Ethernet1/1
    description Trunk to SW-main1
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan
20,30,40,100
    switchport mode trunk
    duplex auto
!

```

```

interface Ethernet1/2
    description Trunk to SW-main3
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan
20,30,40,100
    switchport mode trunk
    duplex auto
!
interface Ethernet1/3
    description Trunk to R2
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan
20,30,40,100
    switchport mode trunk
    duplex auto
!
interface Ethernet2/0
    description Trunk to R1
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan
20,30,40,100
    switchport mode trunk
    duplex auto
!
interface Ethernet2/1
    duplex auto
!
interface Ethernet2/2
    duplex auto
!

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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
    no ip address
    shutdown
    !
interface Vlan20
    ip address 192.168.20.6
    255.255.255.0
    !
interface Vlan100
    ip address 192.168.19.6
    255.255.255.240
    !
    ip default-gateway 192.168.19.3
    !
no ip http server

```

```
control-plane
```

```
!
```

```
!
```

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
line vty 0 4
```

```
login
```

```
!
```

```
end
```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-4 SW-4#sh run Building configuration... Current configuration : 2709 bytes ! ! Last configuration change at 09:20:29 UTC Fri Jun 20 2025 ! version 15.1 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption service compress-config ! hostname SW-4 ! 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 B3YOXN0LhecLa8lIo2gHBzS/hLis8 2ZCDW23dZQIS8U no aaa new-model no ip icmp rate-limit unreachable ! ip cef ! ! no ip domain-lookup ip domain-name corp.local no ipv6 cef ipv6 multicast rpf use-bgp ! spanning-tree mode rapid-pvst spanning-tree extend system-id ! ! vlan internal allocation policy ascending ! ip tcp synwait-time 5 ip ssh time-out 60 ip ssh version 2 ! interface Ethernet0/0 description Trunk to SW-main1 switchport trunk encapsulation dot1q
--	--

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport trunk allowed vlan
20,100
switchport mode trunk
duplex auto
!
interface Ethernet0/1
description Trunk to SW-main3
switchport trunk encapsulation
dot1q
switchport trunk allowed vlan
20,100
switchport mode trunk
duplex auto
!
interface Ethernet0/2
description Workstations -
VLAN 20
switchport access vlan 20
switchport mode access
duplex auto
spanning-tree portfast
!
interface Ethernet0/3
description Workstations -
VLAN 20
switchport access vlan 20
switchport mode access
duplex auto
spanning-tree portfast
!

```

```

interface Ethernet1/0
description Workstations -
VLAN 20
switchport access vlan 20
switchport mode access
duplex auto
spanning-tree portfast
!
interface Ethernet1/1
description Workstations -
VLAN 20
switchport access vlan 20
switchport mode access
duplex auto
spanning-tree portfast
!
interface Ethernet1/2
description Workstations -
VLAN 20
switchport access vlan 20
switchport mode access
duplex auto
spanning-tree portfast
!
interface Ethernet1/3
duplex auto
!
interface Ethernet2/0
duplex auto
!

```

```

interface Ethernet2/1
    ip address 192.168.20.8
    duplex auto
    !
interface Ethernet2/2
    ip address 192.168.20.10
    duplex auto
    !
    no ip http server
    !
interface Ethernet2/3
    duplex auto
    !
    ip access-list standard
    SSH_ONLY
interface Ethernet3/0
    permit 192.168.19.0 0.0.0.15
    duplex auto
    !
    !
    control-plane
interface Ethernet3/1
    !
    duplex auto
    line con 0
    !
    exec-timeout 0 0
interface Ethernet3/2
    privilege level 15
    duplex auto
    logging synchronous
    !
    line aux 0
interface Ethernet3/3
    exec-timeout 0 0
    duplex auto
    privilege level 15
    !
    logging synchronous
interface Vlan1
    line vty 0 4
    no ip address
    access-class SSH_ONLY in
    shutdown
    login local
    !
    transport input ssh
interface Vlan20
    !
    end

```

Скрипти регулярних звітів

Файл 1: Generate-GPOReport.ps1

```

param(

    [string]$ReportPath = "C:\Reports\Security_Reports",

    [string]$DateFormat = "yyyy-MM-dd",

    [string]$FileNameTemplate = "GPO_Report_{0}.txt",

    [bool]$CreateScheduledTask = $false,

    [string]$TaskName = "GPOReportScheduler",

    [string]$Frequency = "Daily",

    [int]$MaxLogSizeMB = 10,

    [int]$MaxLogFiles = 5

)

$reportDate = Get-Date -Format $DateFormat

$gpoReportFile = Join-Path $ReportPath ($FileNameTemplate -f $reportDate)

if (!(Test-Path -Path $ReportPath)) {

    New-Item -ItemType Directory -Path $ReportPath -Force

}

# Log rotation

if (Test-Path $gpoReportFile) {

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

$sizeMB = (Get-Item $gpoReportFile).Length / 1MB

if ($sizeMB -gt $MaxLogSizeMB) {

    $timestamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"

    Rename-Item $gpoReportFile "$gpoReportFile.$timestamp.bak"

}

$files = Get-ChildItem -Path $ReportPath -Filter "*.bak" | Sort-Object
LastWriteTime -Descending

if ($files.Count -gt $MaxLogFiles) {

    $files | Select-Object -Skip $MaxLogFiles | Remove-Item

}

}

try {

    Write-Host "Генерація текстового звіту про GPO..."

    Get-GPO -All | ForEach-Object {

        "Name: $($_.DisplayName)"

        "Status: $($_.GpoStatus)"

        "Created: $($_.CreationTime)"

        "Modified: $($_.ModificationTime)"

        "-----"

    } | Out-File -FilePath $gpoReportFile -Encoding UTF8

    Write-Host "Текстовий звіт про GPO збережено у: $gpoReportFile"

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

$gpoHtmlFile = $gpoReportFile -replace ".txt$", ".html"

Write-Host "Генерація HTML-звіту про GPO..."

Get-GPOReport -All -ReportType Html | Out-File -Encoding UTF8 -
FilePath $gpoHtmlFile

Write-Host "HTML-звіт про GPO збережено у: $gpoHtmlFile"

} catch {

Write-Host "Помилка під час генерації звіту про GPO: $_"

}

if ($CreateScheduledTask) {

try {

$action = New-ScheduledTaskAction -Execute "PowerShell.exe" -
Argument "-NoProfile -File \"\$PSCommandPath\"\"

$trigger = New-ScheduledTaskTrigger -At 2am -Daily

$settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -
DontStopIfGoingOnBatteries -StartWhenAvailable

Register-ScheduledTask -TaskName $TaskName -Action $action -
Trigger $trigger -Settings $settings

Write-Host "Задачу $TaskName створено для автоматичного
запуску."

} catch {

Write-Host "Помилка створення задачі планувальника: $_"

}

}

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

Файл 2: Generate-InactiveUsersReport.ps1

```
param(  
  
    [string]$ReportPath = "C:\Reports\Security_Reports",  
  
    [string]$DateFormat = "yyyy-MM-dd",  
  
    [int]$InactiveDays = 90,  
  
    [string]$FileNameTemplate = "Inactive_Users_Report_{0}.txt",  
  
    [bool]$CreateScheduledTask = $false,  
  
    [string]$TaskName = "InactiveUsersReportScheduler",  
  
    [string]$Frequency = "Daily",  
  
    [int]$MaxLogSizeMB = 10,  
  
    [int]$MaxLogFiles = 5  
  
)
```

```
$reportDate = Get-Date -Format $DateFormat
```

```
$inactiveUsersReportFile = Join-Path $ReportPath ($FileNameTemplate -f  
$reportDate)
```

```
if (!(Test-Path -Path $ReportPath)) {
```

```
    New-Item -ItemType Directory -Path $ReportPath -Force
```

```
}
```

```
# Log rotation
```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

if (Test-Path $inactiveUsersReportFile) {

    $sizeMB = (Get-Item $inactiveUsersReportFile).Length / 1MB

    if ($sizeMB -gt $MaxLogSizeMB) {

        $timestamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"

        Rename-Item                                $inactiveUsersReportFile
"$inactiveUsersReportFile.$timestamp.bak"

    }

    $files = Get-ChildItem -Path $ReportPath -Filter "*.bak" | Sort-Object
LastWriteTime -Descending

    if ($files.Count -gt $MaxLogFiles) {

        $files | Select-Object -Skip $MaxLogFiles | Remove-Item

    }

}

try {

    Write-Host "Аналіз неактивних облікових записів користувачів..."

    $inactiveUsers = Search-ADAccount -AccountInactive -UsersOnly -
TimeSpan (New-TimeSpan -Days $InactiveDays)

    $inactiveUsers | ForEach-Object {

        "Name: $($_.Name)"

        "SamAccountName: $($_.SamAccountName)"

        "LastLogonDate: $($_.LastLogonDate)"

        "Enabled: $($_.Enabled)"

        "DistinguishedName: $($_.DistinguishedName)"

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

"-----"

} | Out-File -FilePath $inactiveUsersReportFile -Encoding UTF8

Write-Host "Текстовий звіт про неактивних користувачів збережено у:
$inactiveUsersReportFile"

} catch {

Write-Host "Помилка під час аналізу неактивних користувачів: $_"

}

if ($CreateScheduledTask) {

try {

$action = New-ScheduledTaskAction -Execute "PowerShell.exe" -
Argument "-NoProfile -File \"\$PSCCommandPath\"\"

$trigger = New-ScheduledTaskTrigger -At 3am -Daily

$settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -
DontStopIfGoingOnBatteries -StartWhenAvailable

Register-ScheduledTask -TaskName $TaskName -Action $action -
Trigger $trigger -Settings $settings

Write-Host "Задачу $TaskName створено для автоматичного
запуску."

} catch {

Write-Host "Помилка створення задачі планувальника: $_"

}

}

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

Файл 3: Generate-SecurityLogReport.ps1

```
param(

    [string]$ReportPath = "C:\Reports\Security_Reports",

    [string]$DateFormat = "yyyy-MM-dd",

    [string]$LogName = "Security",

    [int]$MaxEvents = 1000,

    [string]$FileNameTemplate = "Security_Log_{0}.txt",

    [bool]$CreateScheduledTask = $false,

    [string]$TaskName = "SecurityLogReportScheduler",

    [string]$Frequency = "Daily",

    [int]$MaxLogSizeMB = 10,

    [int]$MaxLogFiles = 5

)

$reportDate = Get-Date -Format $DateFormat

$logReportFile = Join-Path $ReportPath ($FileNameTemplate -f $reportDate)

if (!(Test-Path -Path $ReportPath)) {

    New-Item -ItemType Directory -Path $ReportPath -Force

}

# Log rotation

if (Test-Path $logReportFile) {
```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

$sizeMB = (Get-Item $logReportFile).Length / 1MB

if ($sizeMB -gt $MaxLogSizeMB) {

    $timestamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"

    Rename-Item $logReportFile "$logReportFile.$timestamp.bak"

}

$files = Get-ChildItem -Path $ReportPath -Filter "*.bak" | Sort-Object
LastWriteTime -Descending

if ($files.Count -gt $MaxLogFiles) {

    $files | Select-Object -Skip $MaxLogFiles | Remove-Item

}

}

try {

    Write-Host "Збір подій із журналу $LogName..."

    Get-EventLog -LogName $LogName -Newest $MaxEvents | ForEach-
Object {

        "Time: $($_.TimeGenerated)"

        "EventID: $($_.EventID)"

        "EntryType: $($_.EntryType)"

        "Source: $($_.Source)"

        "Message: $($_.Message)"

        "-----"

    } | Out-File -FilePath $logReportFile -Encoding UTF8

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Write-Host "Текстовий звіт подій збережено у: $logReportFile"

} catch {

    Write-Host ("Помилка під час збору подій з журналу ${LogName}: $_")

}

if ($CreateScheduledTask) {

    try {

        $action = New-ScheduledTaskAction -Execute "PowerShell.exe" -
Argument "-NoProfile -File \"\$PSCCommandPath\"\"

        $trigger = New-ScheduledTaskTrigger -At 4am -Daily

        $settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -
DontStopIfGoingOnBatteries -StartWhenAvailable

        Register-ScheduledTask -TaskName $TaskName -Action $action -
Trigger $trigger -Settings $settings

        Write-Host "Задачу $TaskName створено для автоматичного
запуску."

    } catch {

        Write-Host "Помилка створення задачі планувальника: $_"

    }

}

```

		Шеренгівська О.А.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Миколайчук В.В.				87
Змн.	Арк.	№ докум.	Підпис	Дата		