

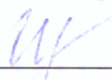
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

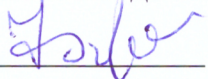
до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект комплексної системи адміністрування та
захисту контролерів домену»

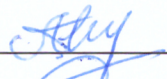
Виконав студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Євгеній ШИТОВ

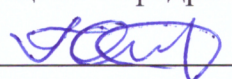
Керівник старший викладач кафедри КІ та КБ

 Ігор ФАЛЬКОВСЬКИЙ

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

 Олексій ШЕЛУХА

Консультант доцент кафедри КІ та КБ, к.пед.н.

 Олена ГОЛОВНЯ

Житомир – 2024 рік

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

“05” 03 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Шитов Євгеній Артемович

Тема роботи: «Проект комплексної системи адміністрування та захисту контролерів домену»

затверджена Наказом університету від 5 березня 2024 р. № 97

Термін здачі студентом закінченої роботи 10.06 2024 р.

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

Об'єктом дослідження є захист IT-інфраструктури Microsoft Active Directory. У процесі виконання кваліфікаційної роботи було розроблено архітектуру системи забезпечення безпеки та адміністрування доменних контролерів. Предметом дослідження є реалізація комплексної системи забезпечення безпеки MS AD. Основна ідея полягає у реалізації захисту активних доменних контролерів від ймовірних атак з сторони кіберзлочинців.

Обладнання та програмне забезпечення:

- мережевий емулятор GNS3, VirtualBox
- операційні системи Windows Server 2019, Windows 10

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

Розділ	Прізвище, ініціали та посади консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1,2,3,4	Головня Олена Сергіївна, доцент кафедри КІ та КБ, к.пед.н.	<u>13.03.2024</u> 	<u>13.03.2024</u> 

Дата видачі завдання “ 6 ” лютого 2024 р

КАЛЕНДАРНИЙ ПЛАН

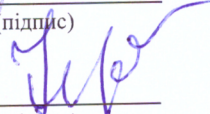
№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2024 02.03.2024 р.	виконано
2	Аналіз літературних джерел	03.03.2024 06.03.2024 р.	виконано
3	Аналіз основних теоретичних відомостей мережевих технологій та Active Directory	07.03.2024- 12.03.2024 р.	виконано
4	Вибір технологій для використання	13.03.2024- 29.03.2024 р.	виконано
5	Створення та налаштування мережі в емуляторі GNS3	30.03.2024- 25.04.2024 р.	виконано
6	Налаштування домену Active Directory	26.04.2024- 05.05.2024 р.	виконано
7	Проведення додаткових налаштувань безпеки доменних контролерів	20.05.2024- 26.05.2024 р.	виконано
8	Написання висновків	07.03.2024- 30.05.2024 р.	виконано
9	Оформлення кваліфікаційної роботи	30.05.2024- 31.05.2024 р.	виконано
10	Підготовка презентації до захисту	Згідно з розкладом	виконано

Студент

Керівник проекту



 (підпис)



 (підпис)

Шитов Є.А
 (прізвище та ініціали)

Фальковський І.Г
 (прізвище та ініціали)

АНОТАЦІЯ

Пояснювальна записка до курсового проекту на тему «Проект комплексної системи адміністрування та захисту контролерів домену» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури.

Текстова частина викладена на 86 сторінках друкованого тексту.

Пояснювальна записка має 4 сторінки додатків. Список використаних джерел містить 29 найменувань і займає 4 сторінки. В роботі наведено 2 таблиці, 95 рисунків. Загальний обсяг роботи – 95 сторінок.

У першому розділі буде проаналізовано поставлене завдання. На основі первинного аналізу задачі визначені необхідні технології.

У другому розділі буде проведено розробку та проектування мережі.

У третьому розділі буде проведений вибір обладнання та налаштування захисту доменних контролерів.

Висновок містить в собі результати виконаної роботи.

У додатку представлені конфігураційні файли.

Ключові слова: MICROSOFT, ACTIVE DIRECTORY, AAA, MFA, CISCO, GNS, NAT, LDAP, SSO, NTLM, NAT.

					ККІКБ.КР.Б – 123 – 20 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект комплексної системи адміністрування та захисту контролерів домену	Літ.		Арк.	Аркушів
Розроб.		Шитов Є.А		12.06.24					
Керівник		Фальковський І.Г		12.06.24				4	95
Реценз.		Шенурок О.О		14.06.24		ФІКТ, Гр. КІ-20-1			
Н. контр.		Фальковський І.Г		12.06.24					
Затверд.		Єфіменко А.А.		14.06.24					

ANNOTATION

The explanatory note to the course project on the topic "Project of a complex system of administration and protection of domain controllers" consists of a list of conventional abbreviations, an introduction, three sections, conclusions, and a list of used literature.

The text part is laid out on 86 pages of printed text.

The explanatory note has 4 pages of annexes. The list of used sources contains 29 names and occupies 4 pages. The work contains 4 tables, 95 drawings. The total volume of work is 95 pages.

In the first section, the task will be analyzed. Based on the initial analysis of the problem, the necessary technologies are determined.

In the second section, the development and design of the network will be carried out.

In the third section, the selection of equipment and the configuration of domain controller protection will be carried out.

The conclusion contains the results of the work performed.

Configuration files are presented in the application.

Keywords: MICROSOFT, ACTIVE DIRECTORY, AAA, MFA, CISCO, GNS, NAT, LDAP, SSO, NTLM, NAT.

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ОПИС ТЕХНОЛОГІЙ СЛУЖБИ ACTIVE DIRECTORY І ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ACTIVE DIRECTORY ДЛЯ НАЛАШТУВАННЯ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ.....	10
1.1. Загальний опис Active Directory	10
1.2 Використання Active Directory для для захисту активних доменних контролерів від атак і взлому	12
1.3 Розгляд можливих спроб проникнення у доменні контролери Active Directory	25
1.4 Постановка технічного завдання	28
РОЗДІЛ 2 ПРОЕКТУВАННЯ НАЛАШТУВАНЬ ЗАХИСТУ АКТИВНИХ ДОМЕННИХ КОНТРОЛЕРІВ НА БАЗІ ACTIVE DIRECTORY, ВИБІР ЗАСОБІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ	30
2.1 Розробка топології комп'ютерної мережі	30
2.2 Розробка схеми адресації мережі.....	31
2.3 Вибір засобів двофакторної аутентифікації	32
2.4 Розгляд використаних технологій захисту та функціоналу Active Directory.....	35
РОЗДІЛ 3 ВСТАНОВЛЕННЯ ТА НАЛАШТУВАННЯ СИСТЕМИ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ НА ОСНОВІ ACTIVE DIRECTORY	40
3.1 Встановлення та налаштування Microsoft Active Directory серверів.....	40
3.2 Встановлення та налаштування двофакторної аутентифікації від Rublon.	71
3.3 Налаштування NAT.....	77
3.4 Відновлення після інцидентів	78
ЗАГАЛЬНІ ВИСНОВКИ	86
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	87
ДОДАТКИ.....	91

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

MS – Microsoft

AD – Active Directory

LDAP – Lightweight Directory Access Protocol

SSO – Single Sign-On

NTLM – NT LAN Manager

MFA – Multi-Factor Authentication

NAT – Network Address Translation

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі, де збереження конфіденційної інформації має вирішальне значення, необхідно розробити комплексну систему захисту та керування контролерами домену. У 2023 та 2024 роках спостерігається значне збільшення кількості зламів доменних контролерів та інших інцидентів з кібербезпеки. Було зафіксовано 3205 інцидентів з порушенням даних, що на 78% більше порівняно з 2022 роком. З цих інцидентів 83% були спричинені зовнішніми атаками, тоді як 19% - внутрішніми порушеннями. Середня вартість одного великого зламу (50-60 мільйонів записів) склала \$332 мільйони у 2023 році. Крім того, витрати на ліквідацію наслідків зламів у сфері охорони здоров'я збільшились на 53.3% з 2020 року, досягнувши в середньому \$10.93 мільйони за один інцидент у 2023 році. Використання безпечної мережі на основі Active Directory є важливим для будь-якої компанії чи організації, оскільки Active Directory забезпечує ефективний механізм для зберігання користувачів, комп'ютерів та інших ресурсів у мережі. Ця система дозволяє контролювати доступ до ресурсів, забезпечує надійний захист від несанкціонованого доступу та знижує ризик розголошення конфіденційної інформації. [\[1\]](#)

Мета кваліфікаційної роботи полягає у ретельному вивченні та аналізі процесу розробки та впровадження складних систем для забезпечення безпеки та керування контролерами домену на основі Active Directory. Крім того, він має на меті вивчити принципи Active Directory як основи безпечної мережі та розглянути практичні аспекти налаштування, моніторингу та обслуговування цієї системи. Результати сертифікаційної роботи містять концептуальні та практичні рекомендації щодо впровадження ефективної та безпечної інфраструктури на основі Active Directory для забезпечення надійного захисту конфіденційної інформації та буде розроблено контрольований доступ до ресурсів в організації.

Об'єктом дослідження є процес розробки захисту IT-інфраструктури Microsoft Active Directory. У процесі виконання кваліфікаційної роботи було розроблено архітектуру системи забезпечення безпеки та адміністрування доменних

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				8
Змн.	Арк.	№ докум.	Підпис	Дата		

контролерів, включаючи налаштування механізмів аутентифікації, авторизації та аудиту доступу.

Предметом дослідження є інструменти та технології комплексної системи забезпечення безпеки MS AD. Основна ідея полягає у реалізації захисту активних доменних контролерів від ймовірних атак з сторони кіберзлочинців.

У процесі виконання кваліфікаційної роботи було розроблено: архітектури системи забезпечення безпеки та адміністрування доменних контролерів, включаючи налаштування механізмів аутентифікації, авторизації та аудиту доступу.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 ОПИС ТЕХНОЛОГІЙ СЛУЖБИ ACTIVE DIRECTORY І ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ACTIVE DIRECTORY ДЛЯ НАЛАШТУВАННЯ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ

1.1. Загальний опис Active Directory

Microsoft Active Directory (AD) - це рішення для керування обліковими записами користувачів, комп'ютерами та іншими ресурсами мережі, розроблене Microsoft. Цей служба каталогу пропонує централізовані можливості автентифікації та авторизації, а також дозволяє адміністраторам керувати доступом до мережевих ресурсів і впроваджувати політики безпеки.

Active Directory зберігає інформацію про різні мережеві об'єкти, такі як користувачі, групи, комп'ютери, принтери та програми. Ця система є масштабованою та може використовуватися для керування ресурсами в доменах або лісах. Адміністратори можуть використовувати групову політику для централізованого керування налаштуваннями для користувачів і комп'ютерів у своїй мережі, включаючи політики безпеки, налаштування робочого столу та встановлення програмного забезпечення.

Active Directory підтримує різні протоколи автентифікації, такі як Kerberos, NTLM і LDAP. Крім того, вона надає функції єдиного входу (SSO) та інтеграції з іншими сервісами Microsoft, такими як Exchange і SharePoint.

Узагальнюючи, можна сказати, що Active Directory є потужним інструментом для керування мережевими ресурсами та надання централізованих послуг автентифікації та авторизації в середовищі Windows. Протокол Kerberos – протокол автентифікації, що використовується для перевірки посвідчення користувача або вузла мережі. Він був розроблений MIT у 1980-х роках і зараз є широко використовуваним протоколом автентифікації для комп'ютерних мереж.[\[2\]](#)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Протокол **Kerberos** використовується для забезпечення безпеки в мережесередовищах через систему на основі квитків, яка автентифікує користувачів і надає доступ до ресурсів. Його робота заснована на обміні зашифрованими квитками між комп'ютером користувача та сервером автентифікації, що забезпечує безпечну автентифікацію та контроль доступу до мережесередовища.

На відміну від Kerberos, протокол NTLM (NT LAN Manager) також використовується для автентифікації користувачів і комп'ютерів у мережевому середовищі Windows. Проте NTLM має свої недоліки у безпеці, такі як вразливість до атак із передачею хешу, що зробило його менш популярним у сучасних середовищах.

У той час як Kerberos і NTLM є протоколами автентифікації, LDAP (Lightweight Directory Access Protocol) використовується для доступу та керування інформацією каталогу, такою як користувачі, групи та ресурси. Цей протокол дозволяє здійснювати пошук та оновлення інформації в ієрархічній структурі каталогу через мережу, що робить його корисним для керування автентифікацією користувачів та доступом до ресурсів у корпоративних та Інтернет-середовищах. [3]

Figure 1: The Kerberos Authentication Process

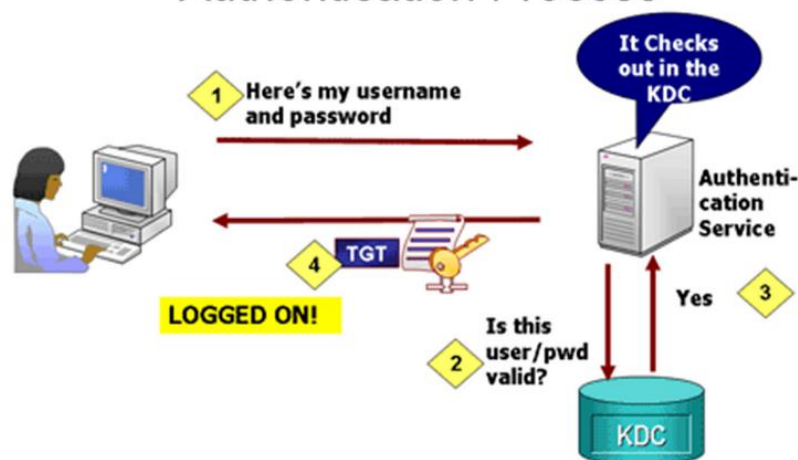


Рис. 1.1.1 Kerberos Authentication Process

1.2 Використання Active Directory для захисту активних доменних контролерів від атак і взлому

Active Directory (AD) є критично важливим інструментом управління ресурсами в середовищі Windows, який надає численні функції для захисту мережі. Захист доменних контролерів, які є серцем мережі Active Directory, вимагає використання різних технологій та підходів. Розглянемо кілька важливих аспектів захисту доменних контролерів за допомогою Active Directory. Розглянемо кілька з них:

- “Автентифікація і авторизація:” - Active Directory надає можливість перевіряти ідентифікаційні дані користувачів і комп’ютерів, які намагаються отримати доступ до мережевих ресурсів, і визначати, до яких ресурсів вони мають доступ. Це дозволяє ефективно контролювати доступ до критичних даних і систем
- “Групова політика (Group Policy):” - дозволяє централізовано налаштовувати параметри безпеки для всіх комп’ютерів у вашій мережі. Забезпечте узгодженість конфігурації та безпеку, щоб запобігти неавторизованим змінам і забезпечити відповідність політикам безпеки.
- “Система доменних імен (DNS):” - Active Directory включає служби DNS для ефективного управління системою доменних імен у мережі, що забезпечує правильну ідентифікацію та доступ до ресурсів.
- “Аудит безпеки:” - Active Directory надає можливість відстежувати та контролювати діяльність користувачів у вашій мережі та запобігати несанкціонованому доступу до ваших ресурсів. Регулярні аудити дозволяють вчасно виявляти потенційні загрози та реагувати на них. [\[4\]](#)

Для захисту доменних контролерів Windows Server можна використовувати різноманітні технології та підходи. Вони мають як свої переваги, так і недоліки. Розберемо їх нижче:

- Firewalls (Брандмауери):

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		12

- Опис: Брандмауери встановлюють бар'єри для мережевого трафіку, що проходить через доменний контролер, контролюючи доступ та фільтруючи небезпечний або небажаний трафік.
- Переваги: Захист від небажаних підключень, зменшення ризику атак.
- Недоліки: Складність конфігурації, можливість блокування легітимного трафіку при неправильному налаштуванні.
- Регулярний аудит та моніторинг:
 - Опис: Проведення регулярного аудиту та моніторингу діяльності доменних контролерів для виявлення та запобігання підозрілої активності.
 - Переваги: Виявлення підозрілої активності на ранніх стадіях. Можливість швидкого реагування на потенційні загрози.
 - Недоліки: Потреба у значних ресурсах для проведення регулярного аудиту. Можливість упущення важливих деталей при великому обсязі даних.
- Централізоване керування доступом:
 - Опис: Системи управління доступом дозволяють налаштовувати права доступу користувачів до різних ресурсів на доменному контролері.
 - Переваги: Гнучке управління доступом, можливість швидко змінювати права доступу.
 - Мінуси: Потреба у складній налаштуванні, можливість виникнення конфліктів у правах доступу.
- Обмеження доступу за географічними ознаками:
 - Опис: Використання географічних обмежень для доступу до доменних контролерів.
 - Переваги: Зниження ризику атак з певних регіонів. Легкість у налаштуванні та управлінні.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Недоліки: Можливість обмеження легітимних користувачів з певних регіонів. Необхідність постійного оновлення списку обмежень.
- Мультифакторна аутентифікація (MFA):
 - Опис: Використання додаткових методів аутентифікації, крім традиційного пароля, таких як ОТР (одноразові паролі), біометричні дані тощо.
 - Переваги: Підвищення рівня безпеки, навіть у випадку витоку паролів.
 - Мінуси: Збільшення складності для користувачів, можливість технічних або людських помилок у процесі аутентифікації.

DNS

Система доменних імен (DNS) має ієрархічну структуру:

1. Кореневий домен:
 - Найвищий рівень.
 - Делегує відповідальність за домени верхнього рівня (TLD).
 - Адмініструється ICANN.
2. Домени верхнього рівня (TLD):
 - Підкоряються кореневому домену.
 - Можуть бути загальними (.com, .org, .net) або географічними (.ua, .ru).
 - Адмініструються різними організаціями.
3. Домени другого рівня:
 - Знаходяться під TLD.
 - Належать компаніям, організаціям або приватним особам.
 - Наприклад, wikipedia.org, example.com.
4. Піддомени:
 - Під доменами другого рівня.
 - Використовуються для групування ресурсів.
 - Наприклад, mail.google.com, support.wikipedia.org.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				14
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Кореневі сервери:

- Авторитетні сервери для кореневого домену.
- Їх IP-адреси публічно доступні.
- Їх кількість обмежена для мінімізації ризиків збоїв.

6. Сервери імен:

- Зберігають записи DNS для конкретних доменів.
- Існують первинні, вторинні та кешуючі сервери.
- Співпрацюють для пошуку IP-адрес доменних імен. [4]

Політика паролів в Active Directory:

Політика паролів в Active Directory (AD) грає критичну роль в забезпеченні безпеки корпоративної мережі. Вона визначає вимоги до створення, використання та зміни паролів для користувачів домену. Основні аспекти політики паролів включають мінімальну довжину пароля, вимоги до складності, термін дії пароля.

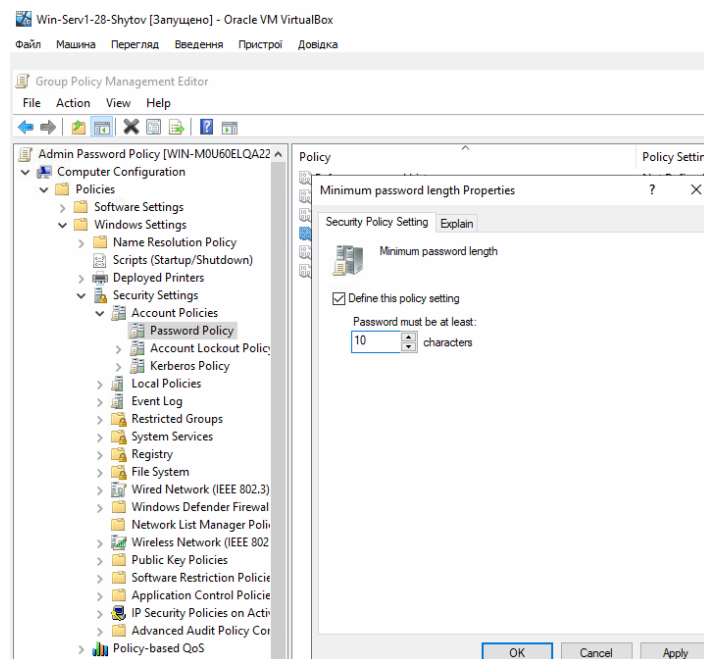


Рис. 1.1.2 Password Policy

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Мінімальна довжина пароля

Мінімальна довжина пароля визначає найменшу кількість символів, яку повинен містити пароль користувача. Це важливий аспект, оскільки коротші паролі є більш вразливими до атак методом перебору.

Вимоги до складності пароля

Вимоги до складності пароля забезпечують, що користувачі створюють паролі, які важче зламати. Складність пароля включає вимогу використовувати комбінацію різних типів символів.

Термін дії пароля

Термін дії пароля визначає, як часто користувачі повинні змінювати свої паролі. Це запобігає використанню одного пароля протягом тривалого періоду, що може збільшити ризик його компрометації.

Історія паролів

Історія паролів запобігає повторному використанню старих паролів користувачами. Це забезпечує, що користувачі не можуть встановити новий пароль таким самим, як один з попередніх паролів. [\[5\]](#)

Політика блокування облікового запису в Active Directory

Політика блокування облікового запису в Active Directory визначає, коли обліковий запис користувача блокується після певної кількості невдалих спроб входу. Ця політика є важливою для захисту облікових записів від атак методом підбору паролів (brute force). Основні параметри політики блокування облікового запису включають кількість невдалих спроб входу, час блокування облікового запису та скидання лічильника невдалих спроб входу.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		16

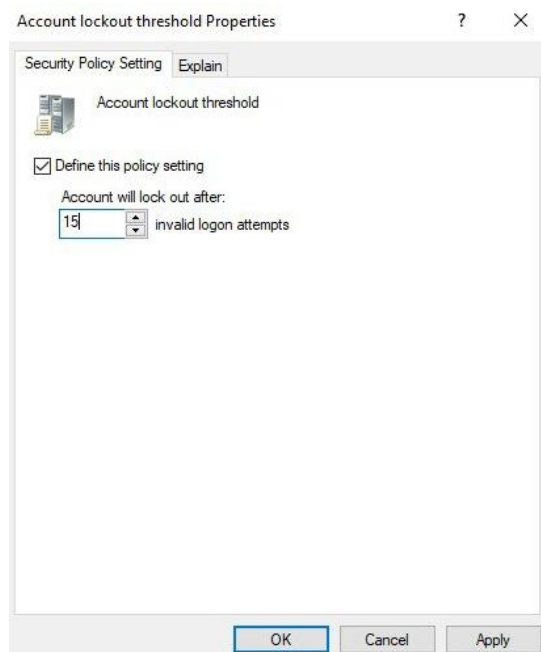


Рис. 1.1.3 Account Lockout

Кількість невдалих спроб входу

Кількість невдалих спроб входу визначає, скільки разів користувач може ввести неправильний пароль до того, як обліковий запис буде заблоковано. Це допомагає захистити обліковий запис від атак методом підбору паролів.

Час блокування облікового запису

Час блокування облікового запису визначає, на який період часу обліковий запис буде заблоковано після досягнення встановленої кількості невдалих спроб входу. Це забезпечує тимчасову неможливість використання облікового запису, що може знизити ризик успішного підбору пароля.

Скидання лічильника невдалих спроб входу

Скидання лічильника невдалих спроб входу визначає, через який час лічильник невдалих спроб входу буде скинуто до нуля, якщо користувач більше не робить спроб входу. Це забезпечує автоматичне відновлення облікового запису після певного періоду. [\[6\]](#)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Налаштування детальної політики паролів в Active Directory

Детальна політика паролів (Fine-Grained Password Policies, FGPP) в Active Directory дозволяє застосовувати різні вимоги до паролів для різних груп користувачів або окремих облікових записів у домені. Це забезпечується за допомогою об'єктів політик паролів (Password Settings Object, PSO). FGPP надає більшу гнучкість в управлінні безпекою паролів, ніж стандартна політика паролів, яка застосовується до всіх користувачів домену.

The screenshot shows the 'Create Password Settings' dialog box. It has a title bar with standard window controls and tabs for 'TASKS' and 'SECTIONS'. The 'Password Settings' section is selected, showing a list of settings. The 'Directly Applies To' section shows a list of users with columns for Name and Mail. The 'Password age options' section includes checkboxes for enforcing minimum and maximum password age, and a section for account lockout policy.

Рис. 1.1.4 Fine-Grained Password Policies

Основні параметри детальної політики паролів

PSO дозволяє налаштовувати ті ж параметри, що і стандартна політика паролів, але на рівні окремих користувачів або груп. Основні параметри включають:

- Мінімальна довжина пароля: Визначає мінімальну кількість символів у паролі.

- Вимоги до складності пароля: Визначає, чи повинен пароль містити символи з різних категорій (великі літери, малі літери, цифри, спеціальні символи).
- Термін дії пароля: Визначає, як часто користувачі повинні змінювати паролі.
- Історія паролів: Запобігає повторному використанню попередніх паролів.

[\[7\]](#)

Інструменти для створення PSO (Password Settings Object)

Для створення та управління об'єктами політик паролів (Password Settings Object, PSO) в Active Directory використовуються різні інструменти, такі як PowerShell та графічні інтерфейси, наприклад, Active Directory Administrative Center (ADAC). Ці інструменти надають адміністраторам гнучкість і зручність в управлінні детальними політиками паролів для окремих користувачів або груп.

- PowerShell - це потужний інструмент для автоматизації завдань і управління конфігураціями в Active Directory. За допомогою PowerShell можна створювати, налаштовувати і призначати PSO швидко та ефективно.
- Active Directory Administrative Center (ADAC) - це графічний інтерфейс для управління об'єктами в Active Directory. Він надає зручний спосіб створення та управління PSO без використання командного рядка. [\[8\]](#)

Реалізація аутентифікації аудиту в Active Directory

Аудит аутентифікації в Active Directory дозволяє відслідковувати і реєструвати спроби входу в систему, а також визначати невдалі спроби входу та інші порушення безпеки. Це є важливим елементом забезпечення безпеки, оскільки дозволяє виявляти і реагувати на потенційні загрози. Основні налаштування аудиту аутентифікації включають моніторинг подій входу в систему, використання облікових даних і виконання привілейованих дій.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Основні компоненти аудиту аутентифікації:

- Вхід в систему (Logon Events)
- Використання облікових даних (Credential Validation)
- Виконання привілейованих дій (Privilege Use)

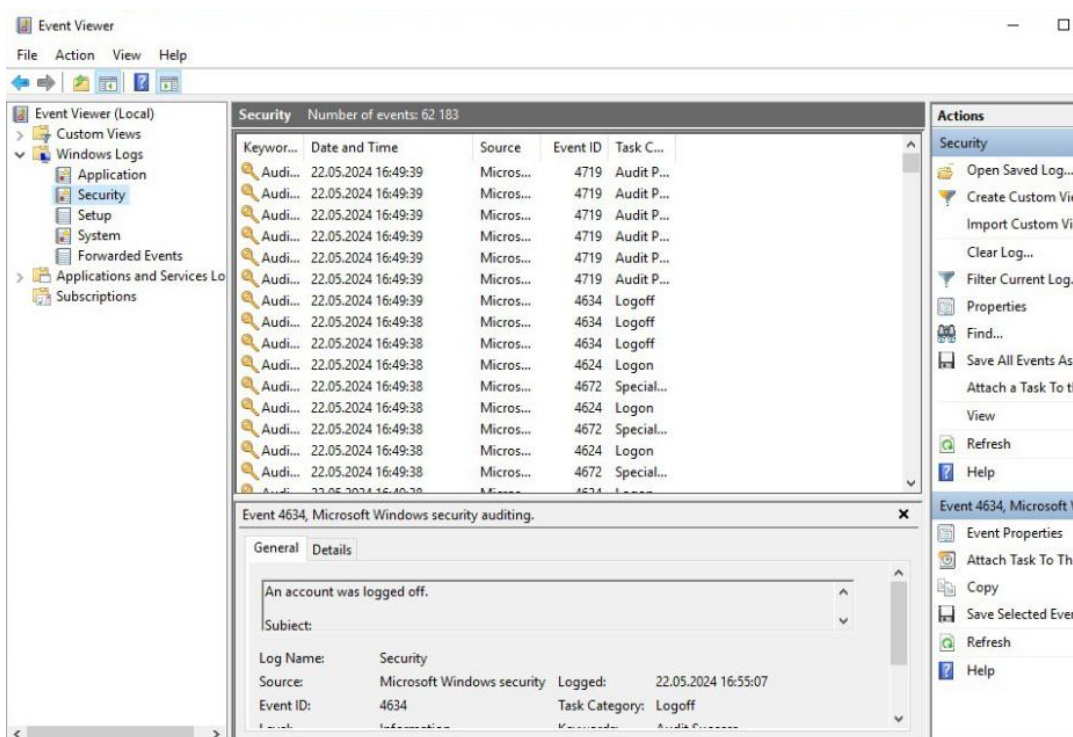


Рис. 1.1.5 Logon Events

Після налаштування аудиту аутентифікації, події будуть записуватись в журнал подій безпеки (Security Event Log) на кожному доменному контролері. Для моніторингу та аналізу подій також можна використовувати такі інструменти як PowerShell. [\[9\]](#)

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				20
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-EventLog -LogName Security -Newest 100

Index Time          EntryType Source                                InstanceID Message
-----
62226 Tpa 22 17:02 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62225 Tpa 22 17:02 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62224 Tpa 22 17:01 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62223 Tpa 22 17:01 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62222 Tpa 22 17:01 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62221 Tpa 22 17:00 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62220 Tpa 22 17:00 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62219 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62218 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62217 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62216 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62215 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62214 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62213 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62212 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62211 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62210 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62209 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62208 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62207 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62206 Tpa 22 16:59 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....
62205 Tpa 22 16:58 SuccessA... Microsoft-Windows... 4634 An account was logged off....
62204 Tpa 22 16:58 SuccessA... Microsoft-Windows... 4624 An account was successfully logged on....

```

Рис. 1.1.6 PowerShell Logon Events

Налаштування облікових записів керованих служб (Managed Service Accounts, MSA)

Керовані облікові записи служб (Managed Service Accounts, MSA) забезпечують автоматичне управління паролями та спрощують адміністрування сервісних облікових записів. Вони створені для автоматизації процесу управління паролями і забезпечення високого рівня безпеки та зручності використання. Основні кроки налаштування включають створення MSA, призначення MSA до служби та оновлення паролів MSA.

```

PS C:\Users\Administrator> Install-ADServiceAccount -Identity EvgeniyMSA
PS C:\Users\Administrator> Test-ADServiceAccount -Identity EvgeniyMSA
True
PS C:\Users\Administrator>

```

Рис. 1.1.7 Встановлення MSA

Переваги використання MSA

- Автоматичне управління паролями: MSA автоматично оновлює свої паролі, що значно зменшує ризик компрометації через використання статичних паролів.
- Підвищена безпека: Паролі MSA оновлюються регулярно і зберігаються в зашифрованому вигляді, що знижує ризики витоку інформації.

- Зручність адміністрування: Спрощується управління сервісними обліковими записами, що зменшує навантаження на адміністраторів.[\[10\]\[11\]](#)

План відновлення після інцидентів (Incident Response Plan)

План відновлення після інцидентів (Incident Response Plan) є важливою складовою системи управління безпекою інформації. Він включає процедури і заходи, необхідні для відновлення роботи системи після виникнення інцидентів, таких як атаки на інформаційну інфраструктуру, втрати даних, або інші серйозні порушення безпеки. Основні компоненти цього плану включають ідентифікацію інцидентів, оцінку впливу, відновлення системи, резервне копіювання та відновлення.

Основні компоненти плану відновлення після інцидентів:

Ідентифікація інцидентів:

- Виявлення і визначення інцидентів безпеки.
- Використання систем моніторингу для виявлення підозрілої активності.
- Документування і класифікація інцидентів за рівнем загрози.

Оцінка впливу:

- Визначення масштабу і впливу інциденту на інформаційну систему.
- Оцінка потенційних збитків і ризиків для організації.
- Визначення пріоритетних дій для мінімізації шкоди.

Відновлення системи:

- Виконання необхідних заходів для відновлення роботи системи.
- Відновлення доступу до критично важливих ресурсів і даних.
- Застосування патчів і оновлень для усунення вразливостей.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Резервне копіювання та відновлення:

- Регулярне створення резервних копій даних і системних конфігурацій.
- Розробка і впровадження процедури відновлення з резервних копій.
- Тестування процесів резервного копіювання і відновлення для забезпечення їх ефективності.[\[12\]](#)[\[13\]](#)[\[14\]](#)

NAT

Network Address Translation (NAT) — це технологія, яка використовується для змінення IP-адрес у заголовках IP-пакетів, що проходять через маршрутизатор або інший пристрій мережевої безпеки. NAT допомагає зменшити кількість необхідних IP-адрес і забезпечує додатковий рівень безпеки для внутрішніх мереж. Статичний NAT (Static NAT) постійно прив'язує одну приватну IP-адресу до однієї публічної IP-адреси. Динамічний NAT (Dynamic NAT) використовує пул публічних IP-адрес, які динамічно призначаються приватним IP-адресам.

Переваги NAT:

- Економія IP-адрес: Зменшує кількість необхідних публічних IP-адрес.
- Безпека: Ховає внутрішню структуру мережі, ускладнюючи атаки ззовні.
- Гнучкість: Полегшує управління IP-адресами у внутрішній мережі.

Недоліки NAT:

- Затримка: Може додавати затримку через трансляцію адрес.
- Сумісність: Деякі протоколи і додатки можуть працювати неправильно.
- Обмеження портів: Кількість одночасних з'єднань обмежена кількістю доступних портів.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		23

NAT працює на мережевому рівні (рівні 3) стека протоколів TCP/IP і зазвичай реалізується в маршрутизаторах або брандмауерах. Це допомагає підвищити безпеку мережі, приховуючи внутрішні IP-адреси пристроїв за однією загальнодоступною IP-адресою, ускладнюючи зовнішнім особам прямий доступ до пристроїв у приватній мережі. [\[15\]](#)

Двофакторна автентифікація, її переваги та методи:

Двофакторна автентифікація – це метод захисту для керування ідентичностями та доступом. Він вимагає дві форми ідентифікації для доступу до ресурсів і даних. Двофакторна автентифікація дає компаніям змогу відстежувати й захищати систему.

Компанії використовують двофакторну автентифікацію, щоб захищати персональні та корпоративні ресурси своїх працівників. Завдяки цьому кіберзлочинці не можуть викрасти або знищити внутрішні записи з даними, а також отримати доступ до них для використання у власних потребах.

Існує безліч переваг двофакторної автентифікації. Наприклад, користувачам не потрібно носити генератор маркерів або завантажувати спеціальну програму для нього. Щоб підтвердити ідентичність на більшості веб-сайтів, користувачі отримують текстові повідомлення на свій мобільний пристрій, приймають виклик або проходять персоналізовану двофакторну автентифікацію.

Нижче наведено деякі інші переваги двофакторної автентифікації:

- Немає необхідності використовувати апаратний генератор маркерів.
Про ці методи двофакторної автентифікації часто забувають. Проте сьогодні їх використовувати зручніше, ніж будь-коли, оскільки технології вдосконалюються.
- Генератори кодів доступу ефективніші, ніж звичайні паролі.
Використовувати генератори безпечніше, оскільки кожен новий код доступу відрізняється від попереднього.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		24

- Завдяки обмеженню на кількість введів коду кіберзлочинці не можуть зламати систему й отримати доступ до делікатних даних.
- Цей процес керований та зручний у використанні.



Рис. 1.1.8 2 Step Autentification

Методи двохфакторної автентифікації:

1. Апаратні маркери
2. SMS-перевірка
3. Push-сповіщення
4. Голосова автентифікація [\[16\]](#)

1.3 Розгляд можливих спроб проникнення у доменні контролери Active Directory

Проникнення (взламування) доменних контролерів на базі Windows Server 2019 може здійснюватися різними методами, кожен з яких експлуатує певні вразливості або недоліки в конфігурації. Найпоширенішими методами проникнення є:

Брутфорс (Brute Force Attack) - атака методом перебору паролів, коли зловмисник пробує велику кількість варіантів паролів для певного облікового запису. [\[17\]](#)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				25
Змн.	Арк.	№ докум.	Підпис	Дата		

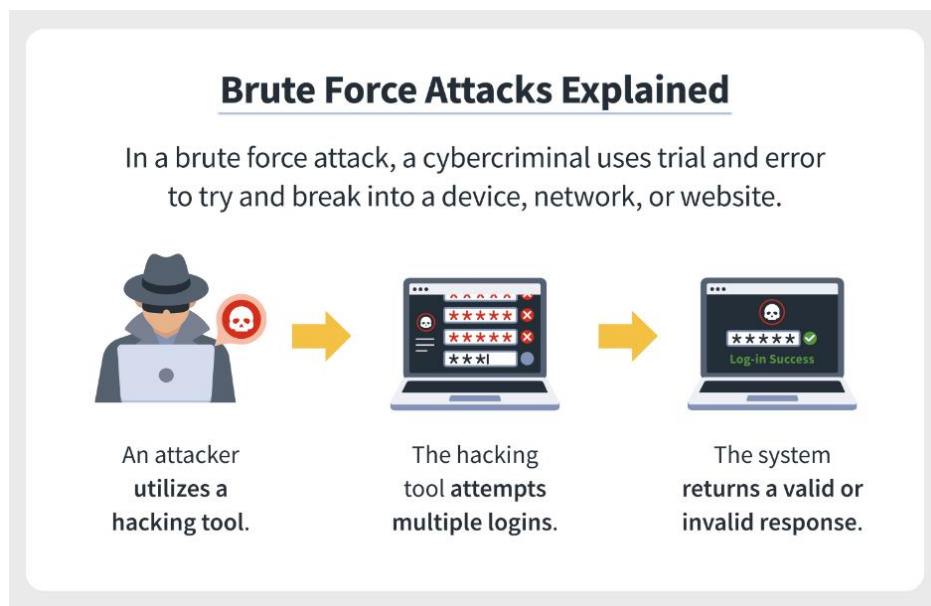


Рис. 1.1.9 Brute Force Attack

Способи захисту - використання складних паролів і вимога їх регулярної зміни, встановлення політики блокування облікового запису після певної кількості невдалих спроб входу а також використання двофакторної аутентифікації (2FA).

Фішинг (Phishing) - зловмисник обманом змушує користувача розкрити свої облікові дані через підроблені веб-сайти, електронні листи або повідомлення.

[\[18\]](#)



When a hacker launches a phishing attack, **he or she is trying to trick you into believing that the message is from a legitimate source** so that you will click a link or download an attachment.

Рис. 1.1.10 Phishing Attack

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Способи захисту – це проведення регулярного навчання для користувачів з питань інформаційної безпеки та використання антифішингових засобів та електронної пошти з підтримкою DMARC, DKIM і SPF.

Pass-the-Hash - зломисник використовує захоплені хеші паролів для аутентифікації без знання паролів. [\[19\]](#)

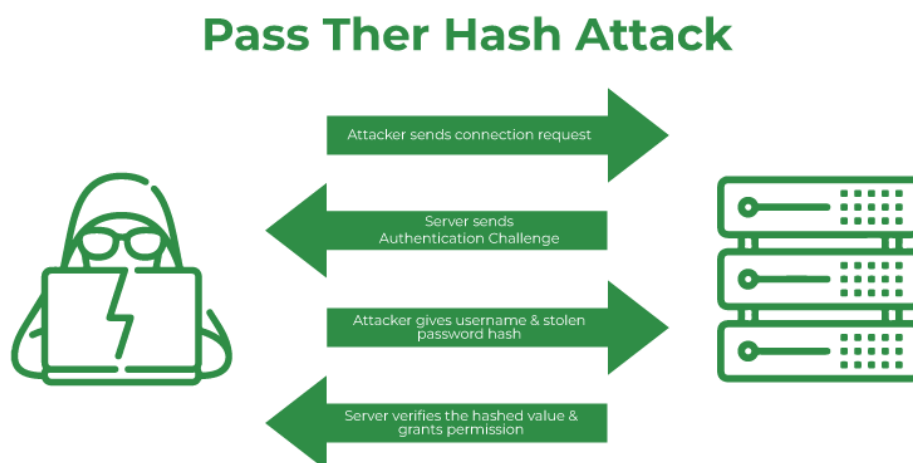


Рис. 1.1.11 Pass-The-Hash Attack

Способи захисту - це впровадження сучасних механізмів аутентифікації (наприклад, Kerberos), використання привілейованих облікових записів тільки на захищених комп'ютерах та регулярне змінювання паролів і хешів.

Атака через віддалений робочий стіл (RDP) - використання відкритих портів RDP для проникнення в систему.

Способи захисту - закриття RDP-портів для зовнішнього доступу або використання VPN та впровадження багатофакторної аутентифікації для RDP.

Віддалене виконання коду (Remote Code Execution - RCE) - використання вразливостей для віддаленого виконання коду на сервері.

Способи захисту - впровадження і налаштування Windows Defender Exploit Guard та використання антивірусного програмного забезпечення з можливістю виявлення RCE-атак. [\[20\]](#)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		27

1.4 Постановка технічного завдання

1. Огляд проекту

Мета проекту - налаштувати захист ІТ на базі рішень Microsoft Active Directory. Проект має на меті забезпечити безпеку та стійкість роботи доменних контролерів, зменшити ризики витоку конфіденційної інформації та відновити доступ до даних у разі непередбачуваних ситуацій.

2. Вимоги до системи

2.1 Функціональні вимоги

- Забезпечення автентифікації користувачів у системі
- Захист конфіденційної інформації
- Моніторинг доступу до системи
- Забезпечення резервного копіювання даних
- Відновлення доступу до даних у разі непередбачуваних ситуацій
- Двофакторна аутентифікація користувачів
- Захист від зловмисних програм
- Доступ до мережі Інтернет
- Наявність MSA

2.2 Нефункціональні вимоги

- Безпека: система повинна бути забезпечена високим рівнем безпеки, забезпечити захист конфіденційної інформації, мінімізувати ризики витоку інформації, відновлювати доступ до даних у разі витоку інформації
- Доступність: система повинна бути доступною в будь-який момент часу, забезпечити безперебійну роботу системи, відновлювати доступ до даних у разі виникнення технічних проблем

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		28

3. Архітектура системи

Система буде базуватися на рішеннях Microsoft Active Directory. В реалізації дозволяється використання будь-яких додаткових технологій для підвищення надійності системи.

Висновки: У першому розділі було проведено детальний огляд технології служби Active Directory, її загальний опис та можливості використання для побудови захищеної мережі. Виявлено, що Active Directory володіє широким спектром функцій, які дозволяють ефективно управляти користувачами, групами та ресурсами в мережі. Серед основних переваг Active Directory виділено централізоване управління доступом, політики паролів, можливості аудиту та захисту від атак. Розглянуто різні методи проникнення у доменні контролери і способи захисту від них, що дозволяє сформулювати комплексну стратегію безпеки для організації.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		29

РОЗДІЛ 2 ПРОЕКТУВАННЯ НАЛАШТУВАНЬ ЗАХИСТУ АКТИВНИХ ДОМЕННИХ КОНТРОЛЛЕРІВ НА БАЗІ ACTIVE DIRECTORY, ВИБІР ЗАСОБІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

2.1 Розробка топології комп'ютерної мережі

Для ІТ-інфраструктури компанії була розроблена топологія захищеної мережі, при проектуванні зверталася увага на наступні моменти:

- Необхідне з'єднання з мережею інтернет
- Наявність робочого домену

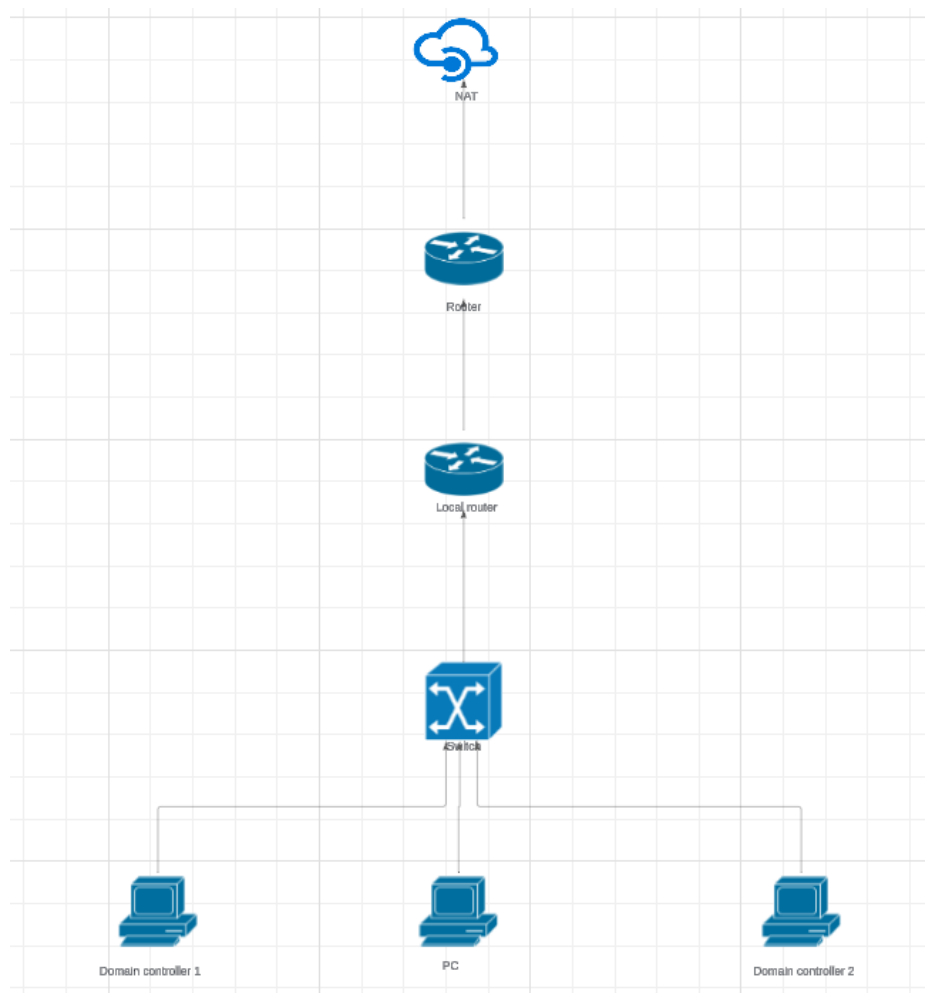


Рисунок 2.1.1 Загальна топологія мережі

Спроектована мережа представлена на рисунку 2.1. Дана мережа складається з 2 маршрутизаторів, 1 комутатора, 2 доменних контролерів.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				30
Змн.	Арк.	№ докум.	Підпис	Дата		

З'єднання між пристроями здійснюється через виту пару Fast Ethernet. Особливістю даного продукту є те, що для підключення комутаційного обладнання використовуються високошвидкісні лінії Fast Ethernet, що забезпечує високу продуктивність мережі. Кінцеві вузли підключаються до комутаційного обладнання за допомогою ланцюгів Fast Ethernet на витій парі.

Адреси кінцевих вузлів отримують через протокол DHCP. Основні політики, розширені паролі та користувачі Active Directory, а також двофакторна автентифікація Rublon використовуються для безпечної автентифікації на мережесхемних пристроях. Для встановлення з'єднання визначено локального користувача. Підключення в основному створюються через користувача адміністратора, створеного на сервері AD.

2.2 Розробка схеми адресації мережі

Як наведено вище, для більшості пристроїв IP адреса буде призначатися автоматично, але всервіно мережа має велику кількість пристроїв, які потребують статично призначені IP адреси. Розрахунки приведені нижче:

Таблиця 2.1 - Інформація про мережу

Призначення	IP-адреса
Мережева адреса:	214.8.29.0
Використовуваний діапазон IP адрес:	214.8.29.1- 214.8.29.30
Широкомовна адреса:	214.8.29.31
Загальна кількість хостів:	30
Кількість доступних хостів:	32
Маска підмережі:	255.255.255.224
Обернена маска:	0.0.0.31
Шлюз по замовчуванню	214.8.29.1

У таблиці 2.1 проведений розподіл IP адрес для усіх мережесхемних пристроїв, адреса шлюзу за замовчуванням є адреса маршрутизатору, адреси серверів.

2.3 Вибір засобів двофакторної аутентифікації

Таблиця 2.2 - Інформація про продукти

Назва продукту	Методи аутентифікації	Цінова політика підписок
Protectimus Winlogon	Time-Based One-Time Password, HMAC-Based One-Time Password, Universal 2nd Factor, Mobile Push, SMS Passcodes	Free, Starter: \$33, Business: \$111, Custom: \$2 на користувача на місяць, Platform: \$199, Cluster: \$299
RSA SecurID	Time-Based One-Time Password, HMAC-Based One-Time Password, Mobile Push, Біометрична аутентифікація, Апаратні токени, PIN-коди.	Cloud: \$2 на користувача на місяць, Cloud Plus: \$4 на користувача на місяць. Cloud Premier: \$6 на користувача на місяць.
Rublon MFA	Mobile Push, Mobile Passcodes, SMS Passcodes, QR Codes, Email Links, WebAuthn/U2F Security Keys, YubiKey OTP	Rublon Free, Rublon Business: \$2 за користувача на місяць, Rublon Enterprise: \$4 за користувача на місяць з мінімумом у 300 ліцензій.

Засоби двофакторної аутентифікації які можна використати для Windows Server:

- Protectimus Winlogon [\[21\]](#)

Двуфакторна аутентифікація для Microsoft RDP & Windows Logon



Рисунок 2.3.1 Protectimus Winlogon

Після встановлення компонента Protectimus Winlogon & RDP на комп'ютер, для входу до свого облікового запису Windows користувачеві потрібно буде пройти два етапи автентифікації: спочатку ввести свій стандартний пароль у Windows, а потім одноразовий пароль, який діє лише 30 секунд.

Двофакторна автентифікація захищає обліковий запис користувача Windows від компрометації у випадку, якщо постійний пароль буде перехоплено, вгадано або зламано за допомогою брутфорсу, соціальної інженерії, фішингу та подібних загроз.

- RSA SecurID [\[22\]](#)

Це апаратне рішення, що використовує токени або картки для генерації одноразових кодів автентифікації.

1. Переваги:

- Висока надійність і безпека.
- Можливість використання безпосередньо без підключення до Інтернету або мобільного зв'язку.

2. Недоліки:

- Високі витрати на обладнання.
- Складність налаштування та управління.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		33



Рисунок 2.3.2 RSA SecurID

- Rublon Autentificator [\[23\]](#)

Rublon - це ще один засіб для двофакторної аутентифікації, який надає рішення для захисту системи.

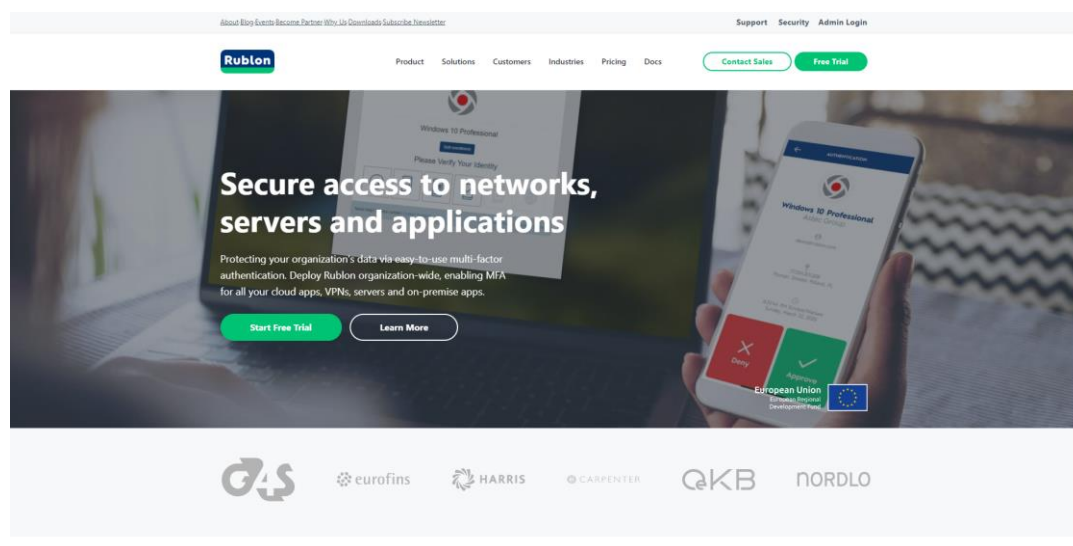


Рисунок 2.3.3 Rublon Autentificator

1. Переваги:

- Легкість використання: Rublon пропонує інтуїтивно зрозумілий інтерфейс для користувачів, що дозволяє легко налаштувати та використовувати систему аутентифікації.
- Безпека: За допомогою Rublon можна надати додатковий рівень безпеки, оскільки він вимагає використання додаткового фактора

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		34

аутифікації, який може бути складніше підібрати, ніж тільки пароль.

- Багатофакторна аутифікація: Rublon підтримує багатофакторну аутифікацію, що дозволяє використовувати кілька методів для підтвердження особи, таких як SMS-повідомлення, мобільний додаток або електронна пошта.

2. Недоліки:

- Вартість: Порівняно з іншими рішеннями для двофакторної аутифікації, Rublon може бути витратним в плані вартості впровадження та управління.
- Залежність від Інтернет-з'єднання: Як і більшість інших засобів для двофакторної аутифікації, Rublon потребує доступу до Інтернету для роботи, що може бути проблематичним у випадку відсутності з'єднання.
- Підтримка: У деяких випадках може виникати проблема з підтримкою або сумісністю з різними системами або пристроями, що може вплинути на його ефективність у конкретному середовищі.

Отже, Rublon може бути оптимальним варіантом для використання у роботі, оскільки він поєднує в собі легкість використання, високий рівень безпеки та підтримку багатофакторної аутифікації, що робить його привабливим рішенням для бізнесу.

2.4 Розгляд використаних технологій захисту та функціоналу Active Directory.

Для створення захищеного користувача (адміністратора) мережі недостатньо лише налаштувати базові політики паролів. Для комфортної і безпечної роботи захисту необхідно реалізувати захисні технології і відповідний функціонал AD.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Для створення захисту буде використаний відповідний функціонал контролеру домену:

- Централізоване керування доступом
- Політика паролів в Active Directory
- Політика блокування облікового запису в Active Directory
- Детальна політика паролів в Active Directory
- Аудит аутентифікації в Active Directory
- Керовані облікові записи служб (Managed Service Accounts - MSA)
- Резервне копіювання даних
- NAT

Централізоване керування доступом

Централізоване керування доступом забезпечує єдину точку управління правами доступу користувачів та груп до різних ресурсів у мережі. В Active Directory це реалізується за допомогою групових політик та надання відповідних дозволів на рівні об'єктів. Наприклад, політика доступу до певних папок або файлів буде встановлюватися через групові політики, що дозволить централізовано контролювати доступ користувачів до конфіденційної інформації.

Політика паролів в Active Directory

Політики групи є основним засобом для визначення вимог до паролів у домені Active Directory. До цього входить налаштування мінімальної довжини пароля, його складність і періоду його чинності. Вимога до користувачів використовувати складні та довгі паролі знижує ймовірність успішності атак методом підбору і, таким чином, ускладнює роботу хакеру.

Політика блокування облікового запису в Active Directory

Щоб запобігти несанкціонованому доступу шляхом повторних спроб підбору пароля, ми встановимо політику блокування облікового запису для

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		36

даного домену. Кількість невдалих спроб входу призводить до автоматичного блокування облікового запису. Групові політики забезпечують можливість налаштування цих параметрів, а також автоматичний захист облікових записів користувача у разі атаки методом підбору.

Детальна політика паролів в Active Directory

Детальна політика паролів (Password Settings Object - PSO) дозволяє застосовувати різні вимоги до паролів для різних груп користувачів або окремих облікових записів. Це реалізується через Password Settings Container в Active Directory Administrative Center. Налаштування PSO допоможе забезпечити високий рівень безпеки для критичних облікових записів, встановлюючи більш суворі вимоги до паролів.

Перевірка аутентифікації в Active Directory

Аудит аутентифікації забезпечує можливість контролю та реєстрації всіх спроб входу до системи. Це сприятиме виявленню та негайній реакції на будь-які підозрілі дії або можливих порушень безпеки. Для налаштування аудиту можна використовувати групові політики, якими визначаються події, що треба реєструвати, наприклад успішні та неуспішні.

Керовані облікові записи служб (Managed Service Accounts - MSA)

Керовані облікові записи служб забезпечують автоматичне управління паролями та спрощують адміністрування сервісних облікових записів. Вони створюються та керуються через PowerShell команди, забезпечуючи безпечне виконання службових завдань без необхідності вручну змінювати паролі.

Резервне копіювання даних

Резервне копіювання є необхідною складовою плану відновлення після інциденту. Щоб забезпечити безпеку даних на доменному контролері, буде увімкнено регулярний автоматичний процес створення резервної копії всіх важливих даних. Це допоможе швидко відновити систему, якщо станеться збій або буде проведена атака. Можливо провести налаштування резервного

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		37

копіювання за допомогою Windows Server Backup або інших програм, призначених спеціально для резервного копіювання.

NAT

На сьогоднішній день кожна локальна мережа має підключення до Інтернету, тому виникає необхідність налаштування підключення до Інтернету. Створена мережа реалізована у GNS3, що вносить певні особливості в її реалізацію. Припустимо, що мережа підключена до комутатора провайдера і отримує адресу через DHCP. Ця адреса дозволяє підключитися до Інтернету, але тільки з одного пристрою. Тому необхідно реалізувати NAT, зокрема динамічний NAT. Використання динамічного NAT обумовлено простотою його налаштування, адже налаштування статичного NAT для всіх вузлів є складним завданням.

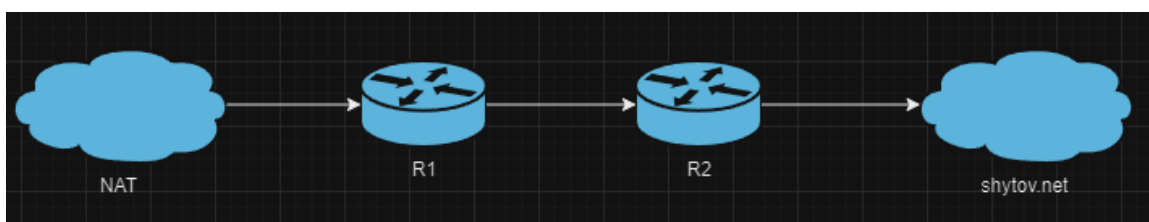


Рис. 2.4.1 Реалізація протоколу NAT

Для реалізації підключення за допомогою NAT буде використано 2 маршрутизатори, маршрутизатор R1 отримає адресу за допомогою протоколу DHCP і даний інтерфейс є NAT outside, а інтерфейс підключений до маршрутизатору R2 має NAT inside. Чому у мережевій схемі використовуються два послідовних маршрутизатори замість паралельного з'єднання для забезпечення надмірності та відмовостійкості?

На це є обґрунтовані причини:

- Розподіл навантаження (R1 може обробляти загальний трафік, тоді як R2 може бути налаштований для роботи з певними сервісами або протоколами.)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Сегментація мережі (R1 може бути використаний для зовнішнього трафіку, а R2 - для внутрішнього, забезпечуючи таким чином розділення зон безпеки.)
- Міграція та тестування (Використання послідовних маршрутизаторів може бути частиною міграційного плану або тестування нових конфігурацій перед тим, як впровадити нову архітектуру паралельно.)

Висновки: Другий розділ був присвячений проектуванню налаштувань захисту активних доменних контролерів на базі Active Directory та вибору засобів двофакторної аутентифікації. В результаті аналізу було розроблено оптимальну топологію комп'ютерної мережі, схему адресації мережі та вибрано найбільш підходящі засоби для забезпечення додаткового рівня безпеки за допомогою двофакторної аутентифікації. Проведено порівняння різних технологій двофакторної аутентифікації, таких як Protectimus Winlogon, RSA SecurID та Rublon, з детальним описом їх переваг та недоліків.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		39

РОЗДІЛ 3 ВСТАНОВЛЕННЯ ТА НАЛАШТУВАННЯ СИСТЕМИ ЗАХИСТУ ДОМЕННИХ КОНТРОЛЕРІВ НА ОСНОВІ ACTIVE DIRECTORY

3.1 Встановлення та налаштування Microsoft Active Directory серверів Налаштування захисту активних доменних контролерів

Для початку роботи з AD сервером необхідно його встановити, тому почнемо з встановлення AD серверу. Встановлення серверу подібно до встановлення звичайної ОС Windows, розбиремо лише основні моменти.

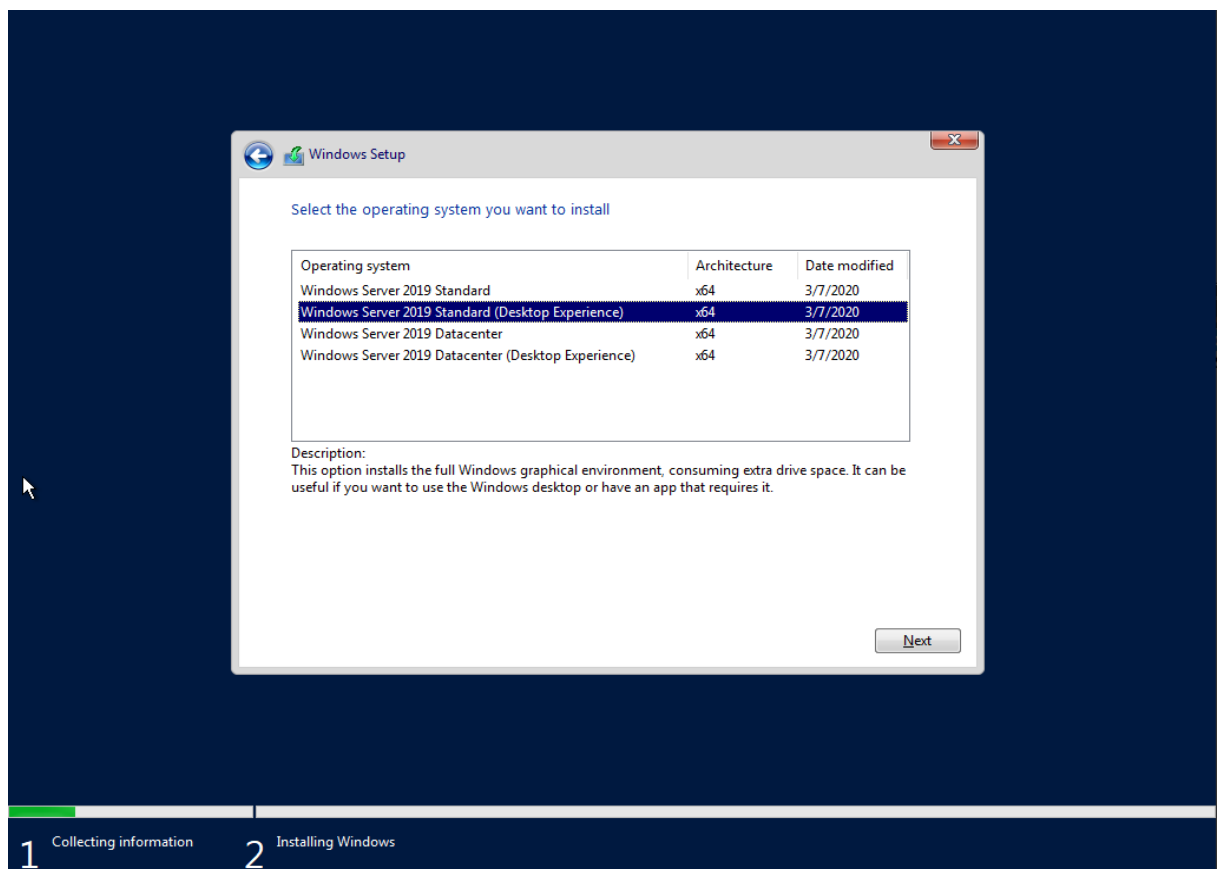


Рис. 3.1.0 Вибір ОС для встановлення

Важливим моментом є вибір ОС для встановлення, важливо розуміти чим відрізняються запропоновані для встановлення ОС, нам необхідні ОС Windows Server 2019 Standard. Windows Server 2019 Standard і Windows Server 2019 Standard (Desktop Experience) відрізняються наявністю графічного інтерфейсу, відсутність графічного інтерфейсу може бути плюсом за обмежених ресурсів для серверу, у нашому випадку ресурсів для серверу достатньо і наявність

графічного інтерфейсу набагато спрощую роботу з сервером, тому встановлюємо Windows Server 2019 Standard (Desktop Experience). Windows Server 2019 Datacenter та Windows Server 2019 Standard (Desktop Experience) відрізняються віртуалізацією (Datacenter підтримує необмежену кількість віртуальних машин, тоді як Standard обмежений до двох), функціями зберігання (Datacenter включає повну підтримку Storage Spaces Direct, Storage Replica, Deduplication, а Standard - ні), мережевими можливостями (Datacenter має повну підтримку SDN, якої немає в Standard), Shielded Virtual Machines (доступні тільки в Datacenter) і Advanced Threat Protection (включена в Datacenter, але відсутня в Standard). Проблема Windows Server 2019 Datacenter полягає у вимогливості до апаратної частини та дороговизни ліцензування. [24]

Далі вибираємо тип встановлення Custom: Install Windows only (advanced).

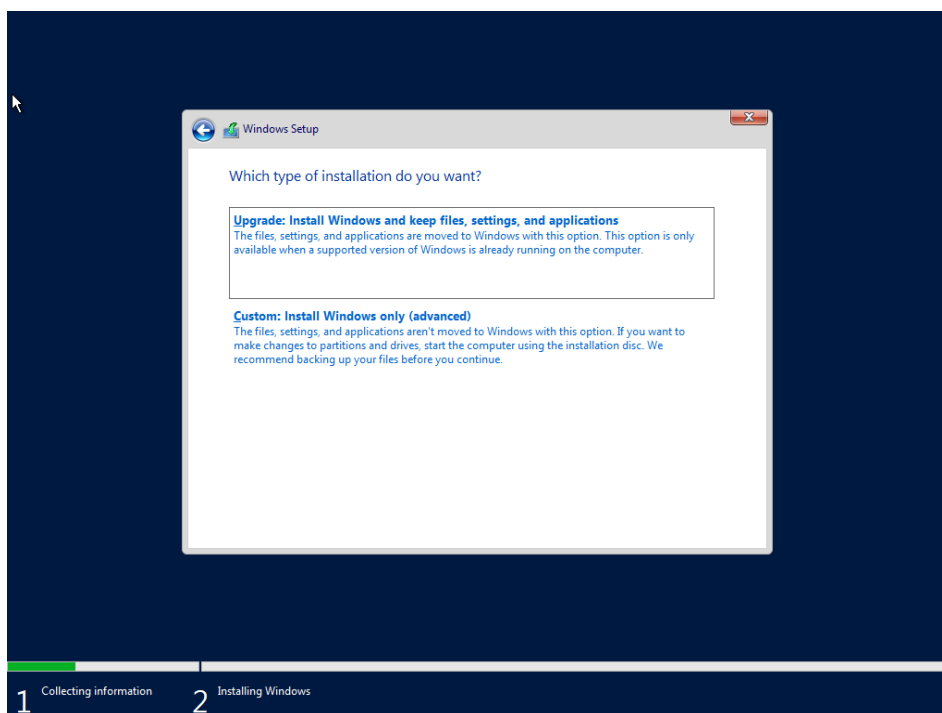


Рис. 3.1.1 Вибір типу встановлення

Далі перейдемо до розділення жорсткого диска. Цей розділ дозволяє керувати доступним простором на жорсткому диску, формувати жорсткий диск і розділяти його на томи. У нашому випадку ми створимо один том для всього вільного простору.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		41

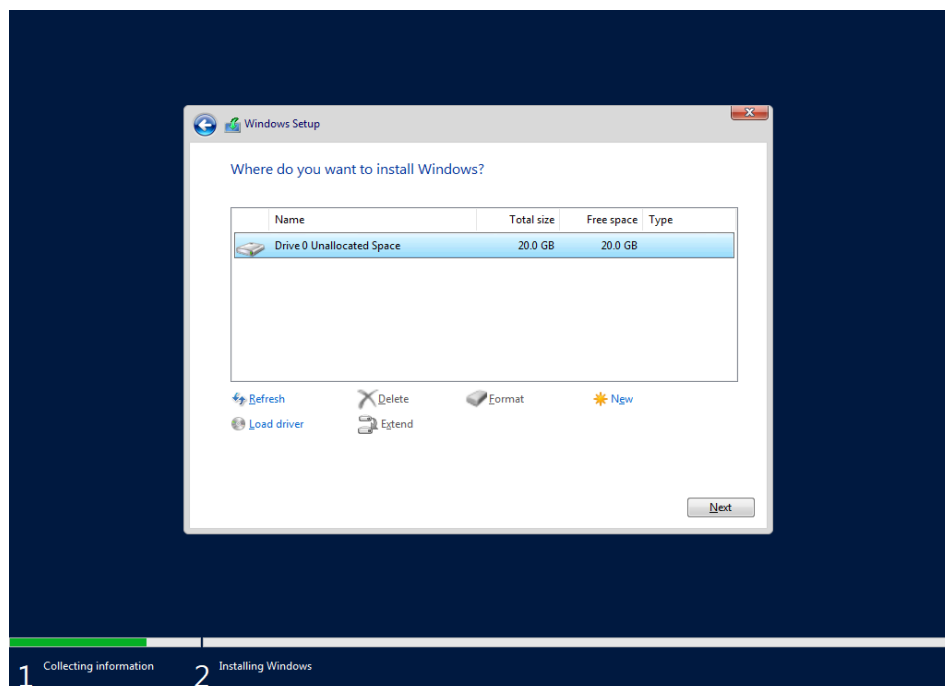


Рис. 3.1.2 Розбиття диску

Далі чекаємо встановлення серверу і можемо переходити до налаштувань самого Active Directory серверу.

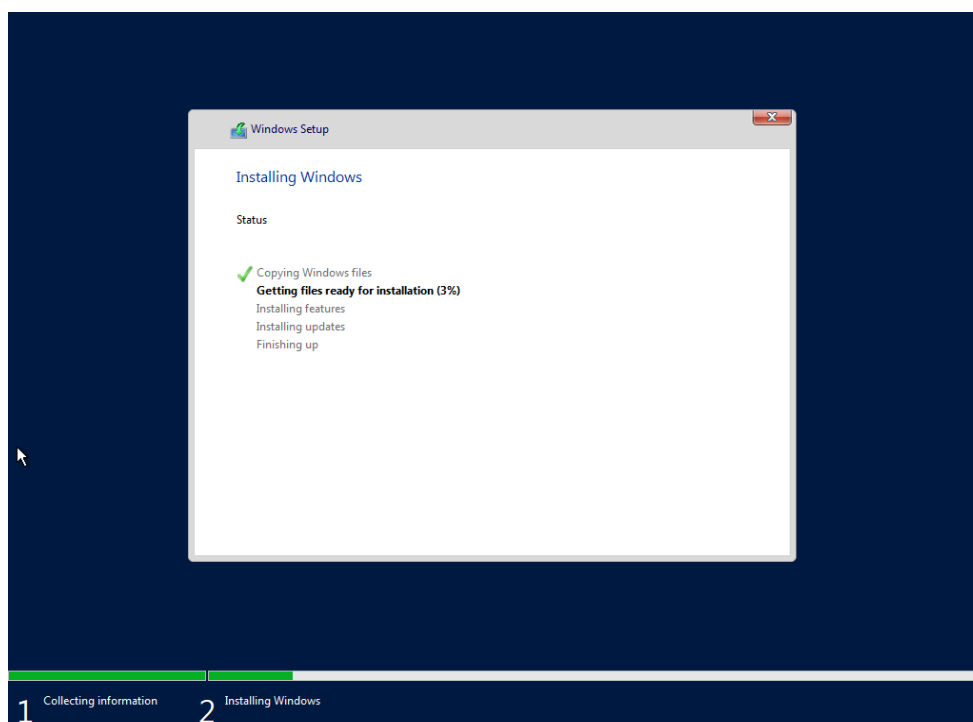


Рис. 3.1.3 Процес встановлення AD серверу

Перед розгортання серверу як контролер домену необхідно провести базові налаштування системи:

- налаштування IP адресації (сервер має мати статичну адресу)
- налаштувати назву серверу (за потреби)
- налаштування часу (часового поясу)

Після базової конфігурації можна самостійно розгорнути контролери домену. Додавати модулі, необхідні для роботи домену можна по мірі виконання роботи. Тому спочатку інсталуємо лише доменні служби Active Directory.

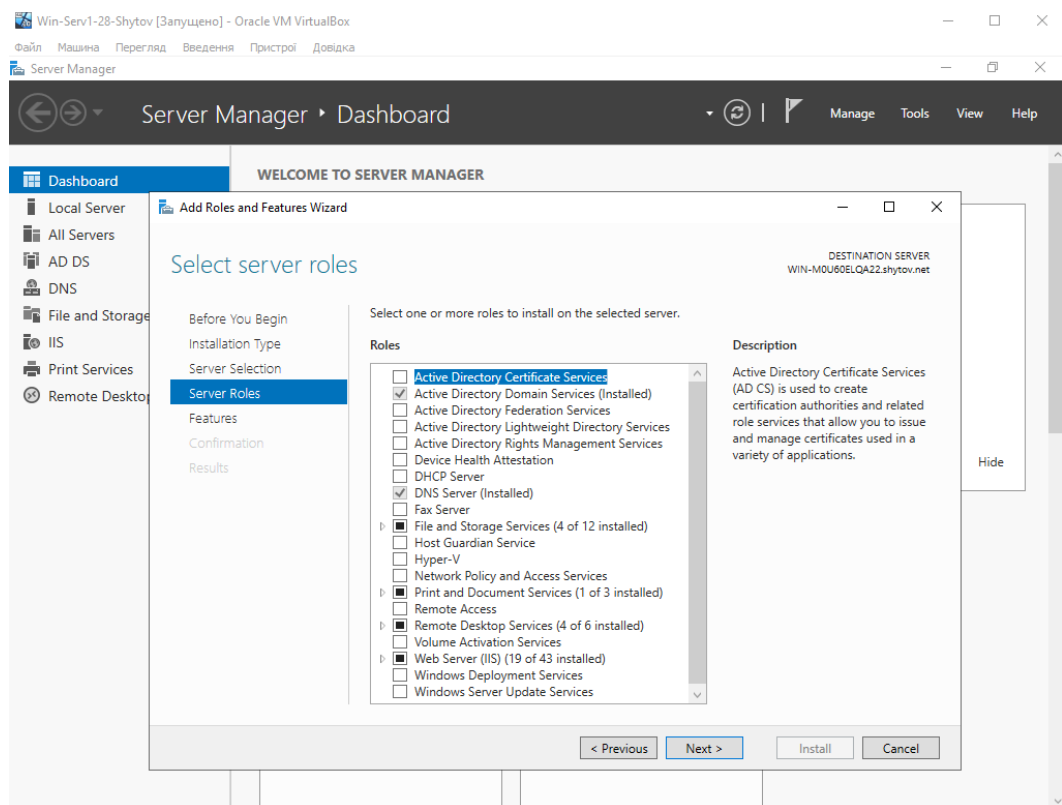


Рис. 3.1.4 Вибір модулів для встановлення

Після встановлення модуля розгортаємо цей сервер як контролер домену, вибираємо відповідний пункт і вводимо назву домену.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		43

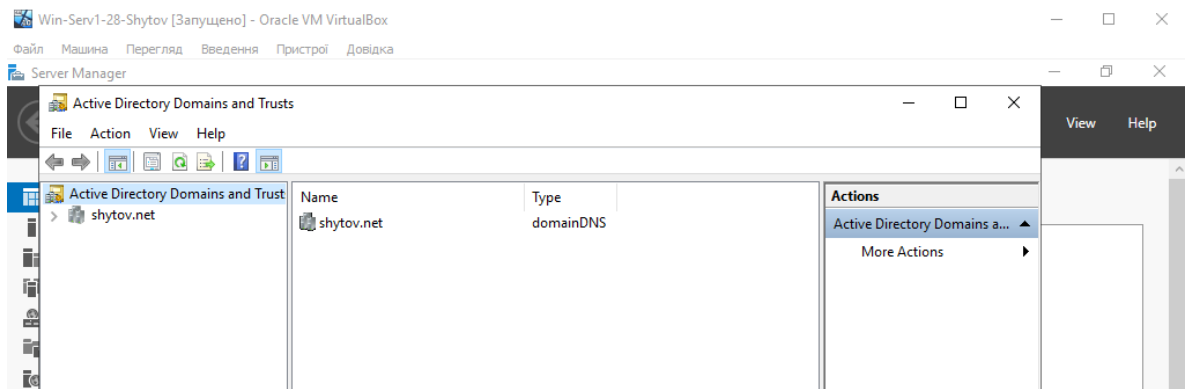


Рис. 3.1.5 Розгортання серверу як контролер домену

Задаємо пароль і вибираємо функціональний рівень контролеру домену.

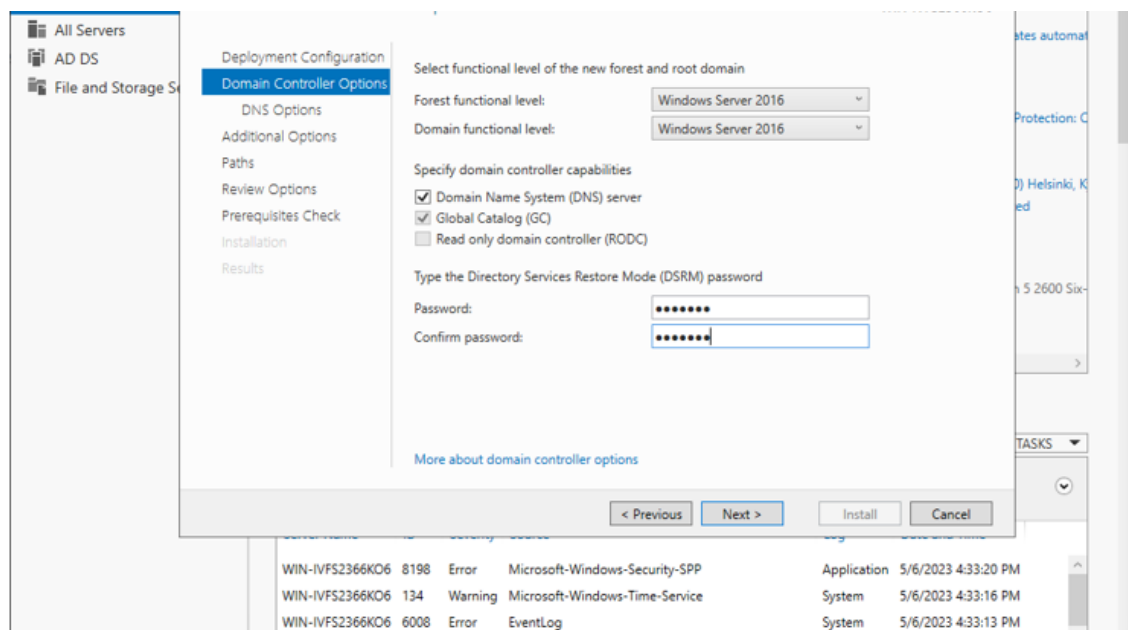


Рис. 3.1.6 Вибір функціонального рівня та задання паролю

Налаштування DNS на базі AD серверу

Для того щоб у нас працював і домен і інтернет нам потрібно провести певні налаштування. Для роботи нам необхідно встановити:

- DNS

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		44

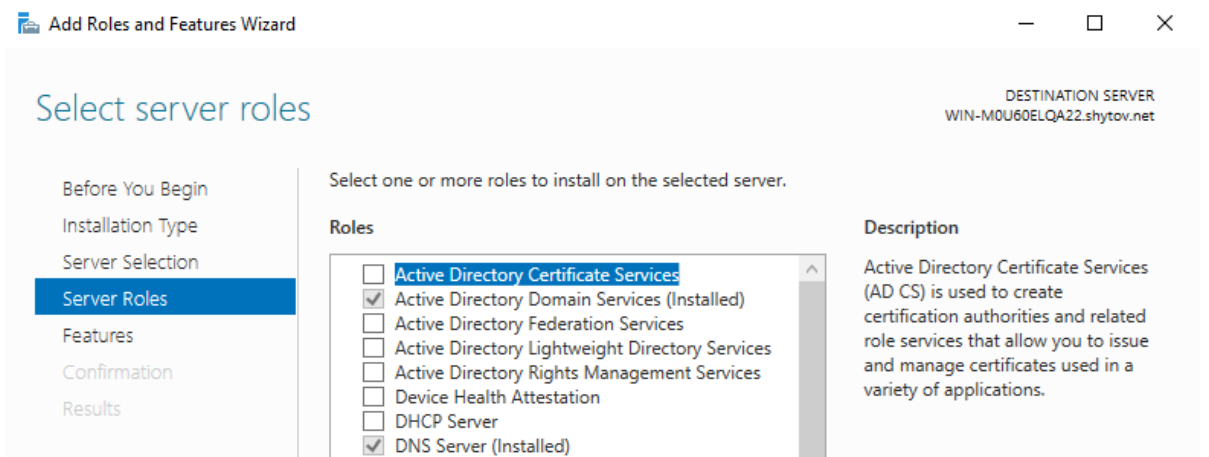


Рис. 3.1.7 Встановлення необхідних модулів

Далі переходимо до створення запису DNS

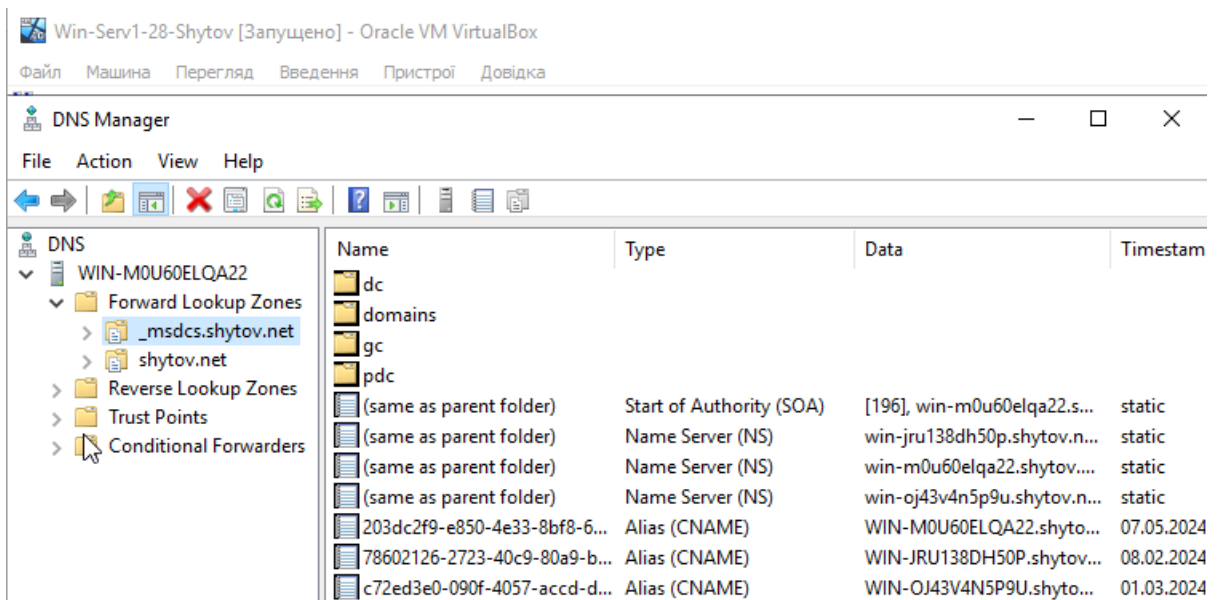


Рис. 3.1.8 Створені записи

Далі переходимо до налаштування Active Directory DNS, а саме до налаштування адресації.

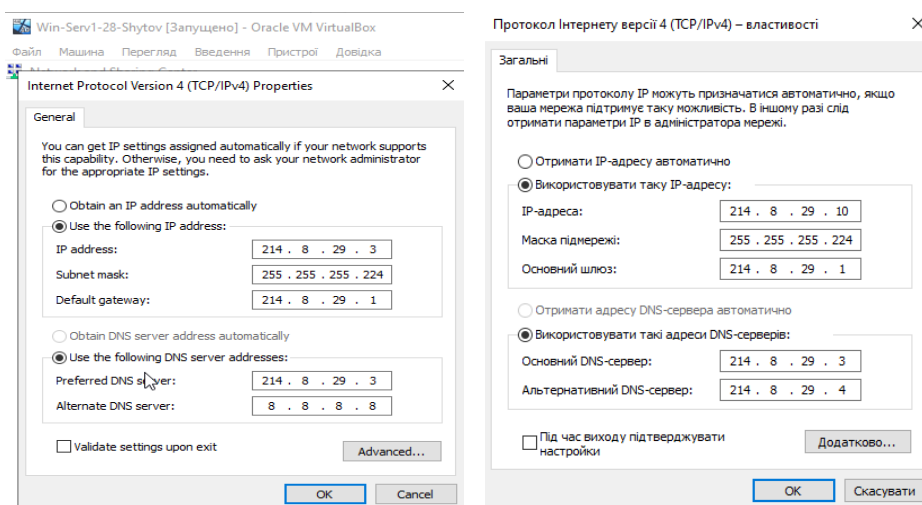


Рис. 3.1.9 Налаштування DNS

Для коректної роботи з мережею Інтернет було налаштовано пересилання пакетів DNS. Пересилання пакетів DNS виконує функцію відправлення DNS пакетів на зовнішній DNS сервер за відсутності відповідного хоста у базі основного DNS серверу.

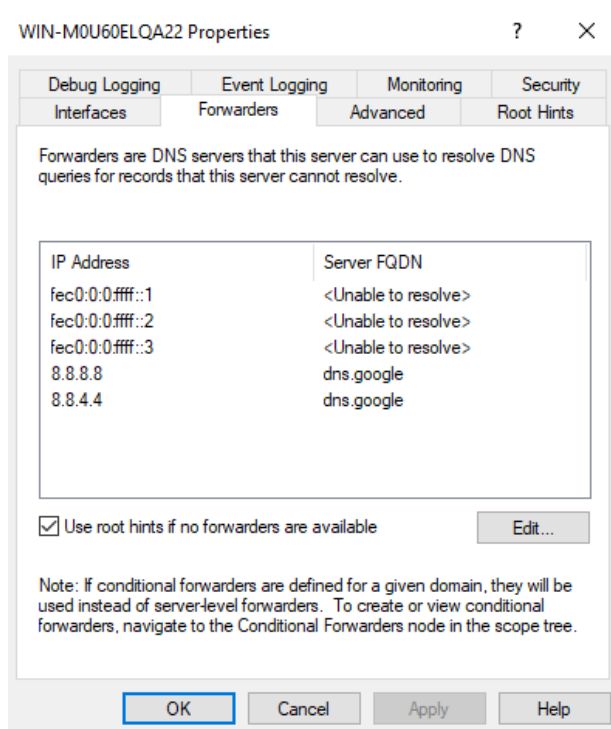


Рис. 3.1.10 Налаштування пересилання пакетів

Додавання робочої станції до домена

Додаємо нову робочу станцію до домену, для цього переходимо у властивості ПК > Налаштування імені комп'ютера, домену та робочої групи > Змінити налаштування.

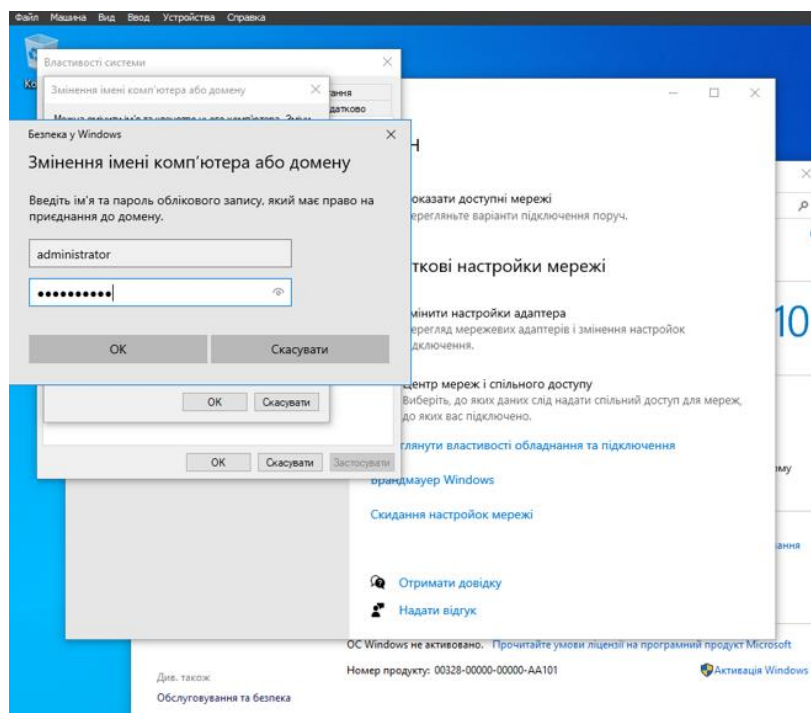


Рис. 3.1.11 Додавання робочої станції до домена

За необхідності змінюємо ім'я робочої станції та вводимо назву домену, після введення паролю користувача адміністратора приєднуємося до домена.

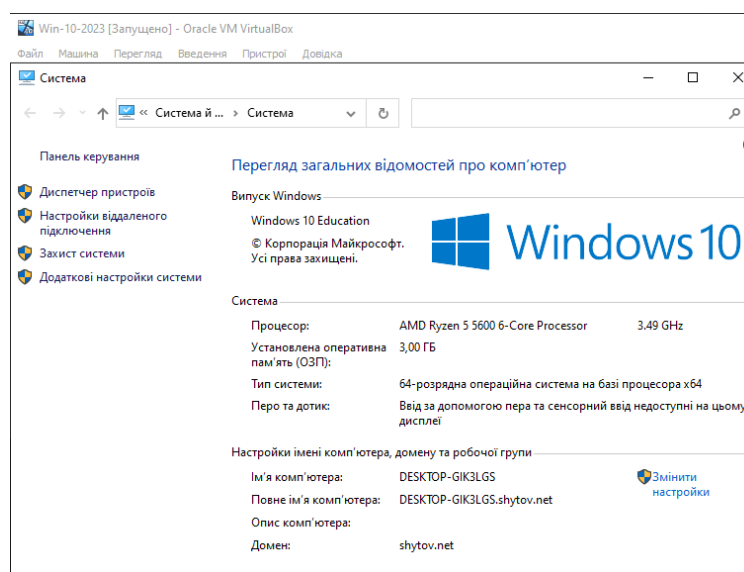


Рис. 3.1.12 Успішне приєднання до домена

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Налаштування базової політики паролів

Надійні паролі є важливим елементом безпеки, оскільки вони запобігають несанкціонованому доступу до системи. Слабкі паролі легко можуть бути зламані атакуючими за допомогою різноманітних методів, таких як перебір спроб, словники або використання програмних засобів для злому паролів. В результаті слабких паролів ризик порушення безпеки збільшується.

Для початку потрібно створити групи користувачів і дати їм певні права:

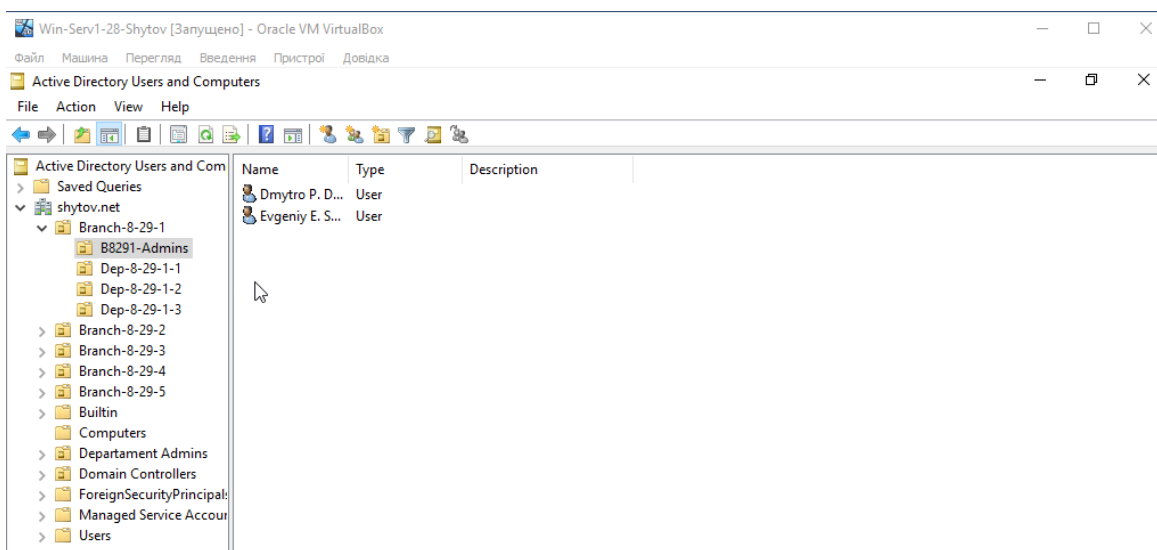


Рис. 3.1.13 Створення користувачів

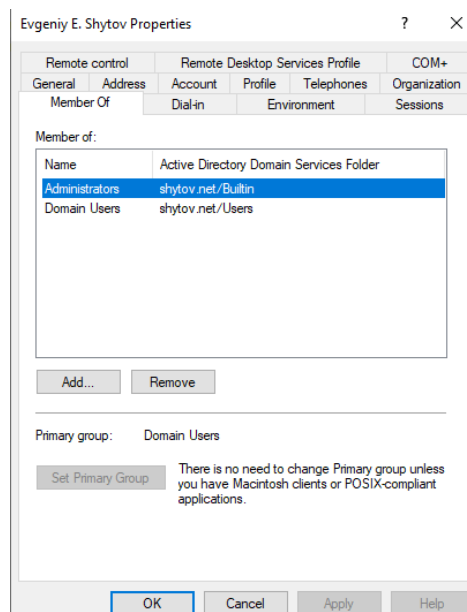


Рис. 3.1.14 Надання прав користувачам

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				48
Змн.	Арк.	№ докум.	Підпис	Дата		

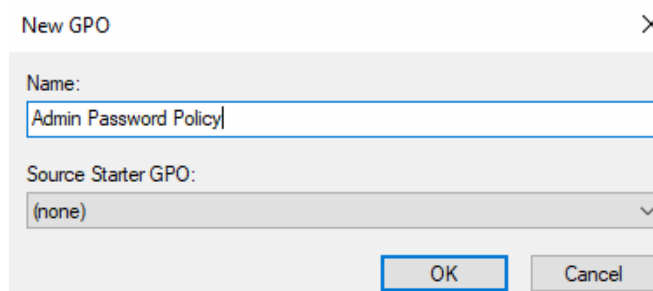


Рис. 3.1.15 Встановлення GPO

Далі налаштовуємо мінімальну довжину паролю:

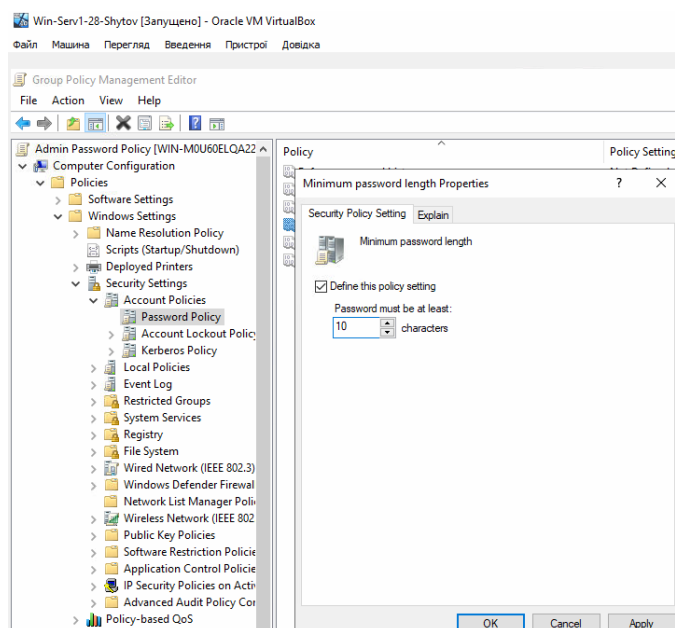


Рис. 3.1.16 Встановлення довжини паролю

Після цього можемо приступати до задання часового проміжку зміни паролю:

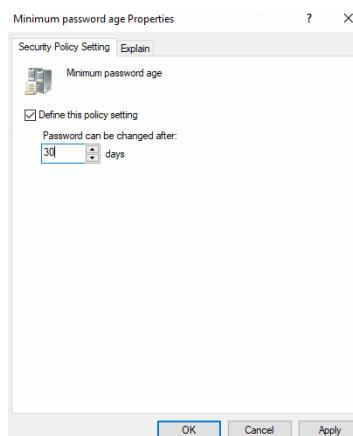


Рис. 3.1.17 Проміжок життя паролю

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Блокування користувачів

Це налаштування використовується для визначення кількості невдалих спроб входу в систему, після яких обліковий запис користувача буде заблоковано.

Для виконання налаштувань використаємо Group Policy Management Editor:

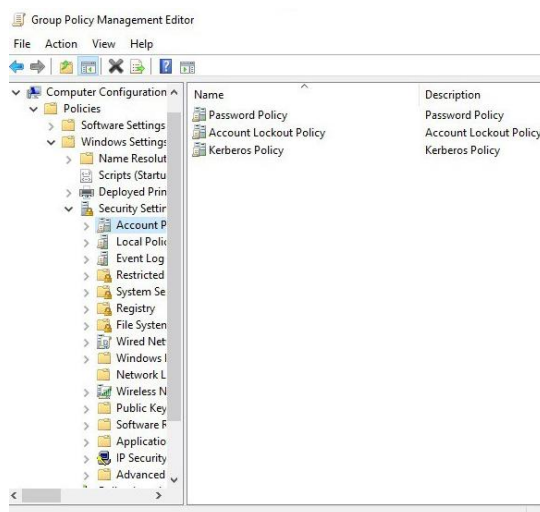


Рис. 3.1.18 Group Policy Management Editor

Оберемо кількість невдалих спроб входу, необхідних для блокування облікового запису:

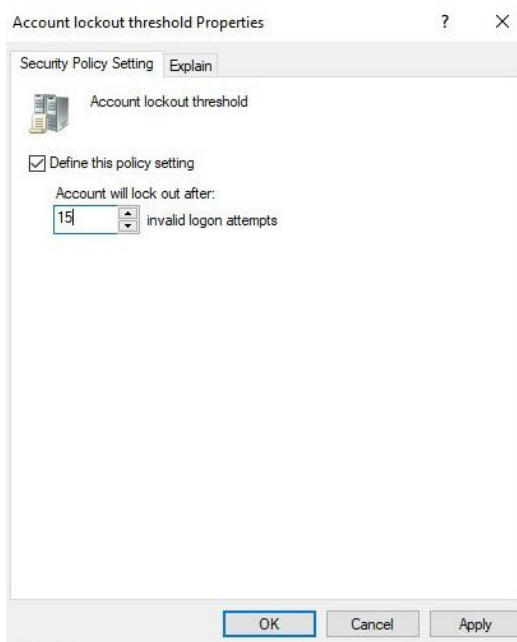


Рис. 3.1.19 Account lockout threshold Properties

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Обираємо час блокування аккаунту після 15-ти неуспішних спроб входу в обліковий запис:

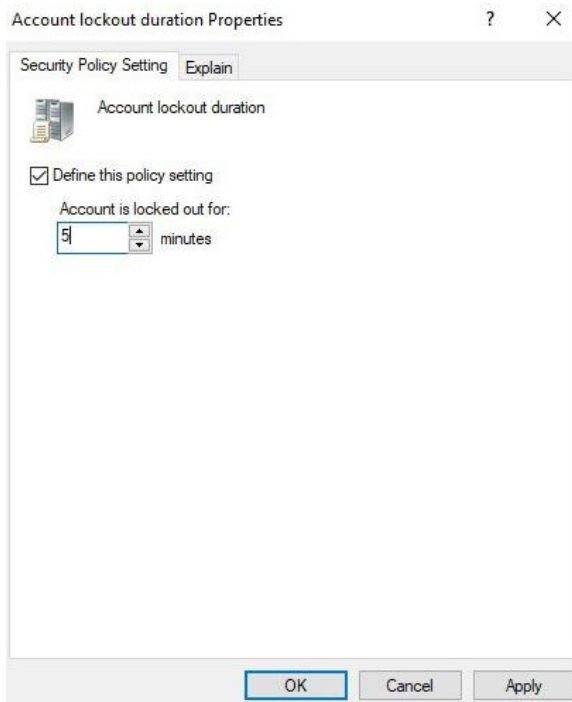


Рис. 3.1.20 Account lockout duration Properties

Обираємо час скидання лічильника невдалих спроб входу:

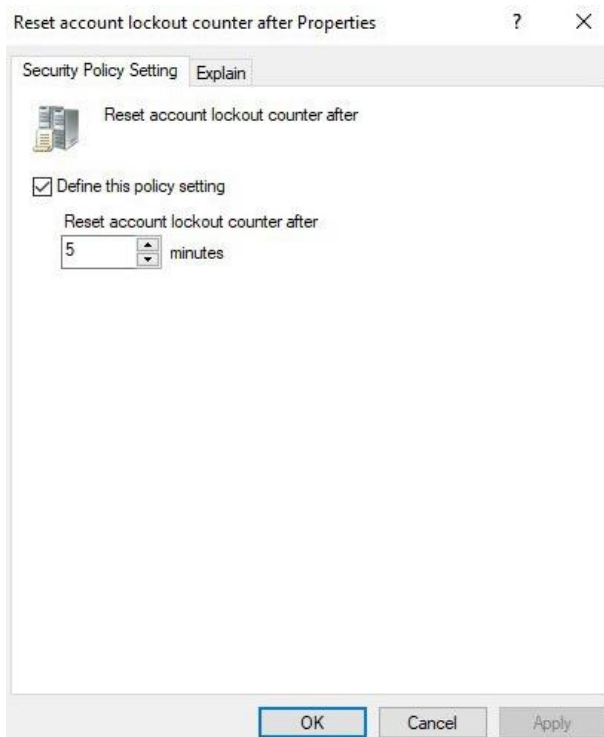


Рис. 3.1.21 Account lockout counter after Properties

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування детальної політики паролів у Windows Server 2019

Щоб перейти до налаштувань детальної політики паролів потрібно використати Active Directory Administrative Center (Центр адміністрування Active Directory). Цей інтерфейс використовується для управління налаштуваннями паролів в Active Directory, такими як політики складності паролів, вимоги до довжини пароля, термін дії пароля та інші параметри, які допомагають забезпечити безпеку і зручність управління обліковими записами користувачів в домені.

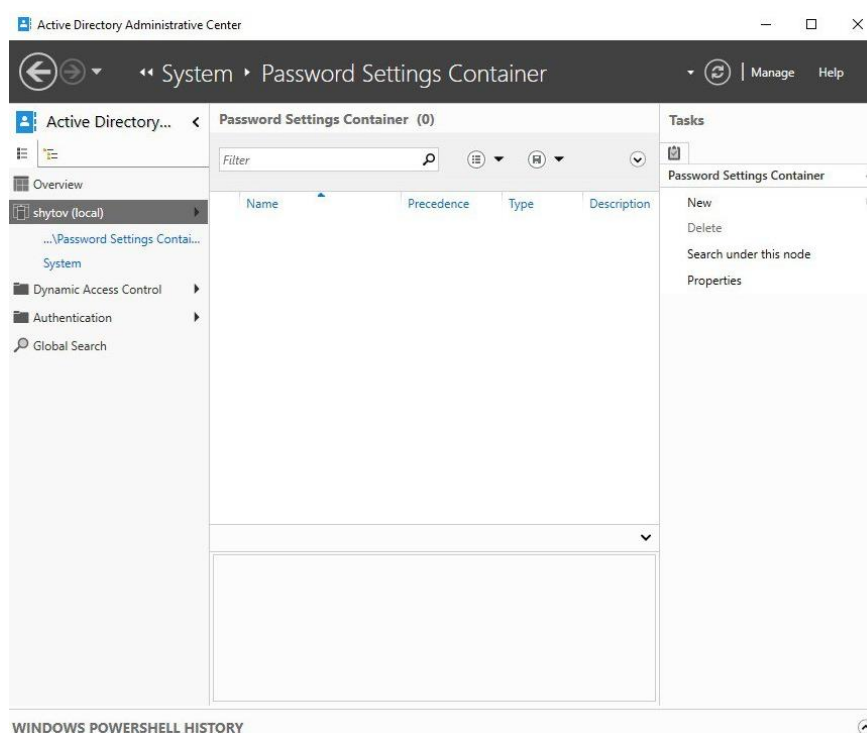


Рис. 3.1.22 Active Directory Administrative Center

У гілці Password Settings Container обираємо New для створення нової політики. Перед нами спливає вікно детальних налаштувань політик паролів:

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		52

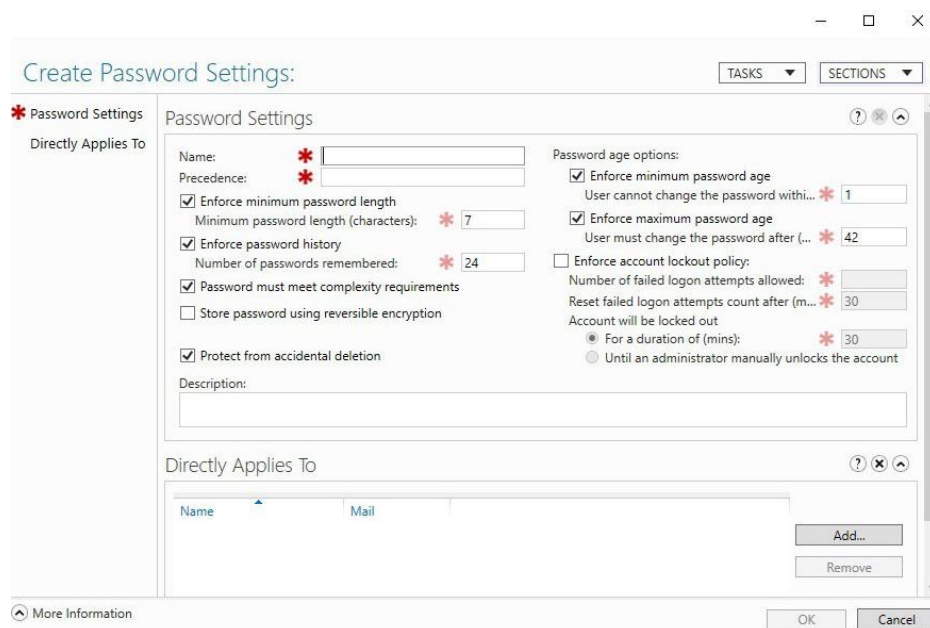


Рис. 3.1.23 Create Password Settings

На зображенні показано вікно створення налаштувань пароля (Create Password Settings) в Active Directory Administrative Center (Центр адміністрування Active Directory). Це вікно дозволяє адміністраторам налаштовувати політику паролів для користувачів в домені.

Основні елементи:

Ліва частина вікна:

- Password Settings (Налаштування паролів) - активна вкладка.
- Directly Applies To (Застосовується безпосередньо до) - вкладка для вказівки об'єктів, на які застосовуються налаштування.

Центральна частина вікна:

- Name (Ім'я): Поле для введення назви налаштування пароля.
- Precedence (Пріоритет): Поле для введення пріоритету налаштування.
- Enforce minimum password length (Примусове встановлення мінімальної довжини пароля): Опція з введенням мінімальної довжини пароля (7 символів).

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				53
Змн.	Арк.	№ докум.	Підпис	Дата		

- Enforce password history (Примусове збереження історії паролів): Опція з введенням кількості запам'ятовуваних паролів (24).
- Password must meet complexity requirements (Пароль повинен відповідати вимогам складності): Опція для забезпечення складності паролів.
- Store password using reversible encryption (Зберігати паролі з можливістю зворотного шифрування): Опція для зберігання паролів у зворотному шифруванні.
- Protect from accidental deletion (Захист від випадкового видалення): Опція для захисту налаштування від видалення.

Опції віку паролів (Password age options):

- Enforce minimum password age (Примусове встановлення мінімального віку пароля): Опція з введенням мінімального часу, протягом якого користувач не може змінювати пароль (1 день).
- Enforce maximum password age (Примусове встановлення максимального віку пароля): Опція з введенням максимального часу, протягом якого користувач повинен змінити пароль (42 дні).

Політика блокування облікових записів (Enforce account lockout policy):

- Number of failed logon attempts allowed (Кількість дозволених невдалих спроб входу): Опція з введенням кількості дозволених невдалих спроб входу (30).
- Reset failed logon attempts count after (minutes) (Скидання кількості невдалих спроб входу через (хвилини)): Опція з введенням часу скидання лічильника невдалих спроб (30 хвилин).

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		54

- Account will be locked out (Обліковий запис буде заблоковано): Опція з вибором тривалості блокування облікового запису (30 хвилин або до ручного розблокування адміністратором).

Нижня частина вікна:

- Directly Applies To (Застосовується безпосередньо до): Секція для додавання об'єктів (користувачів або груп), до яких застосовуються ці налаштування пароля. Кнопки "Add" (Додати) та "Remove" (Видалити).

Верхня частина вікна:

Кнопки "Tasks" (Завдання) та "Sections" (Секції) для додаткових опцій і налаштувань.

Після аналізу вікна проводимо необхідні нам налаштування:

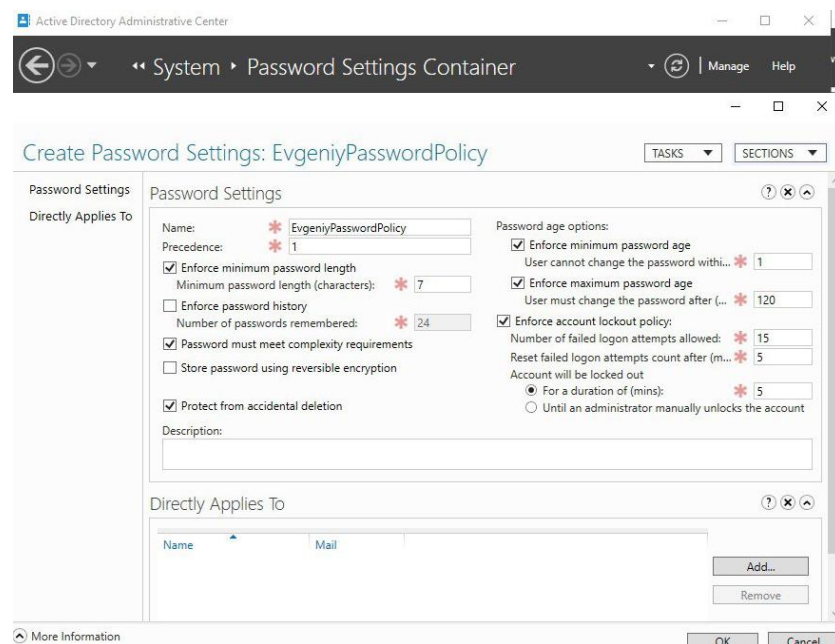


Рис. 3.1.24 Create Password Settings (Обрані налаштування)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				55
Змн.	Арк.	№ докум.	Підпис	Дата		

Обираємо користувачів або групи для яких буде застосовано політику:

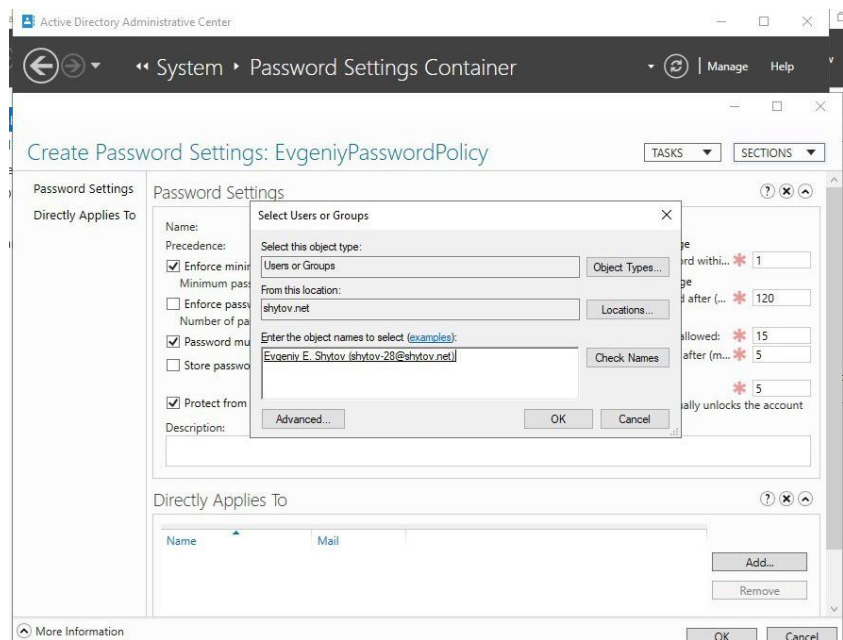


Рис. 3.1.25 Обрання користувачів або груп

Після проведених налаштувань на виході отримуємо готову та робочу політику (EvgeniyPasswordPolicy)

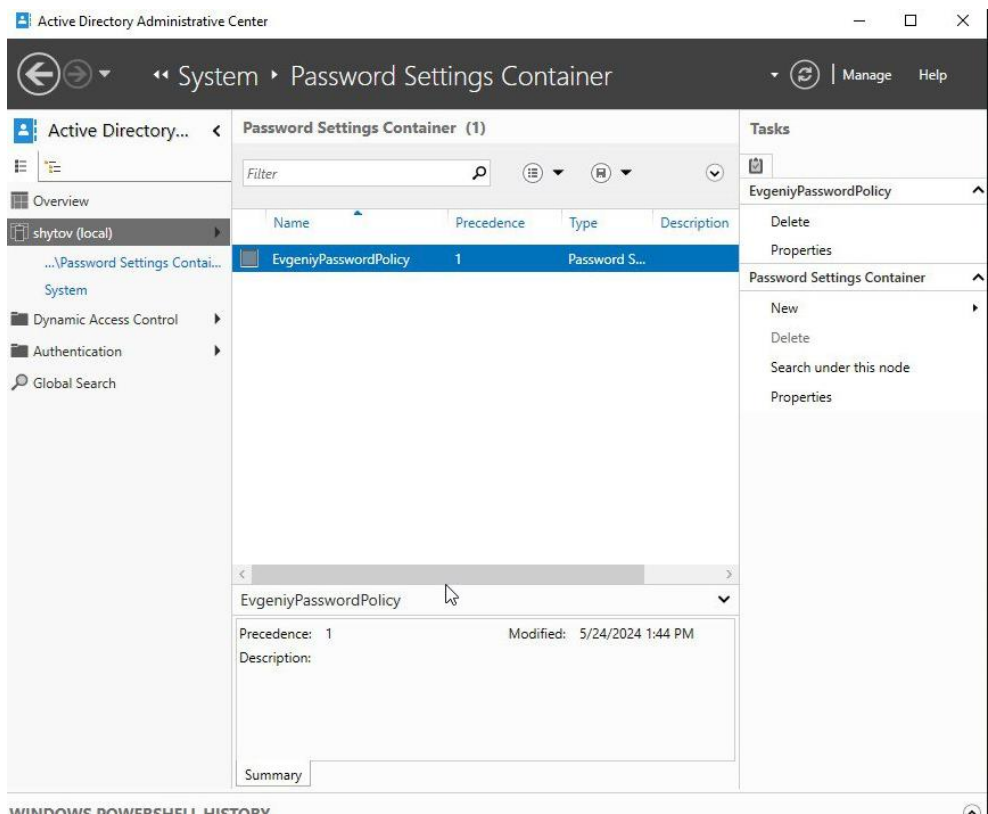


Рис. 3.1.26 Створена політика

Налаштування аудитів входу-виходу(Event Viewer)

Для того щоб події коректно відображалися у аудитах входу і виходу потрібно провести певні налаштування. Спочатку обираємо рядки "Audit Account Lockout","Audit Logoff", "Audit Logon" і встановлюємо значення "Success and Failure" (Успіх і Помилка).

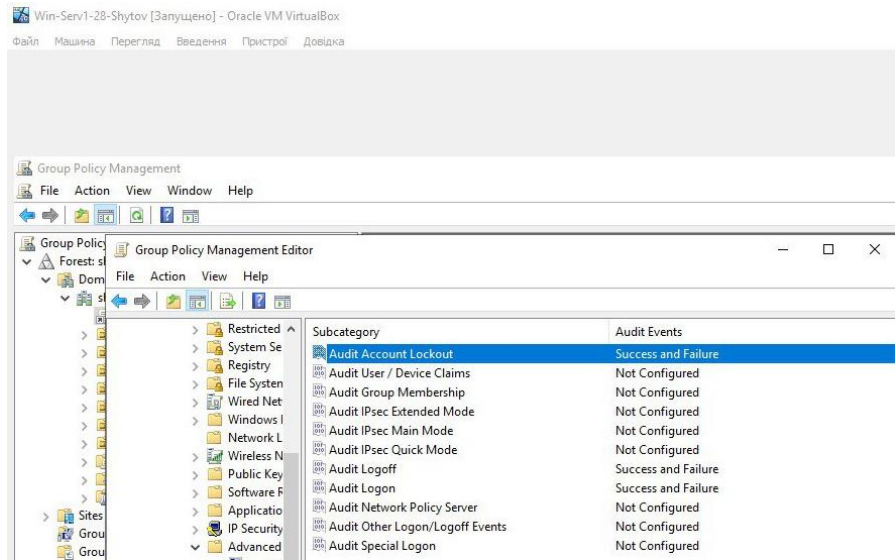


Рис. 3.1.27 Audit Events

Обираємо потрібні нам пункти (успішно,неуспішно).

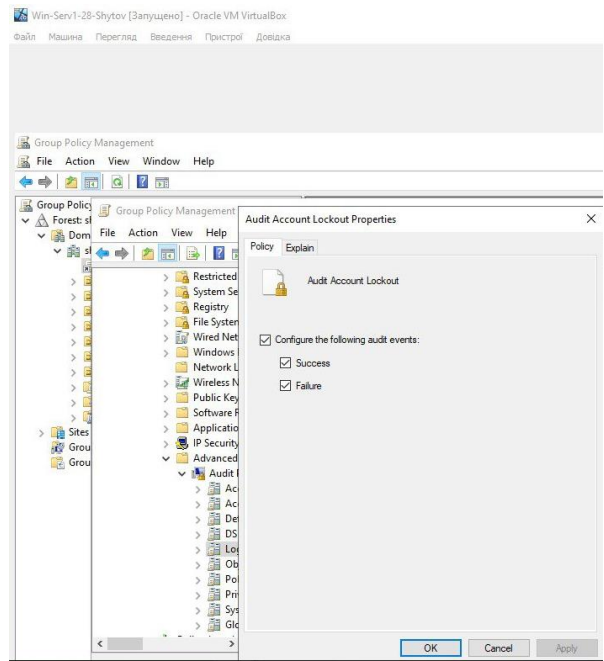


Рис. 3.1.28 Audit Account Lockout Properties

Такі самі налаштування проводимо і для двох залишившихся пунктів.

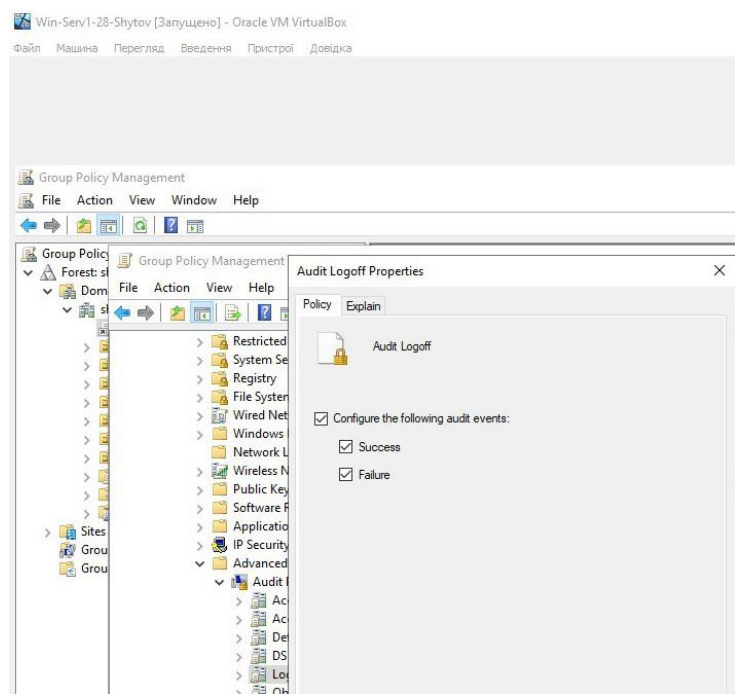


Рис. 3.1.29 Audit Logoff Properties

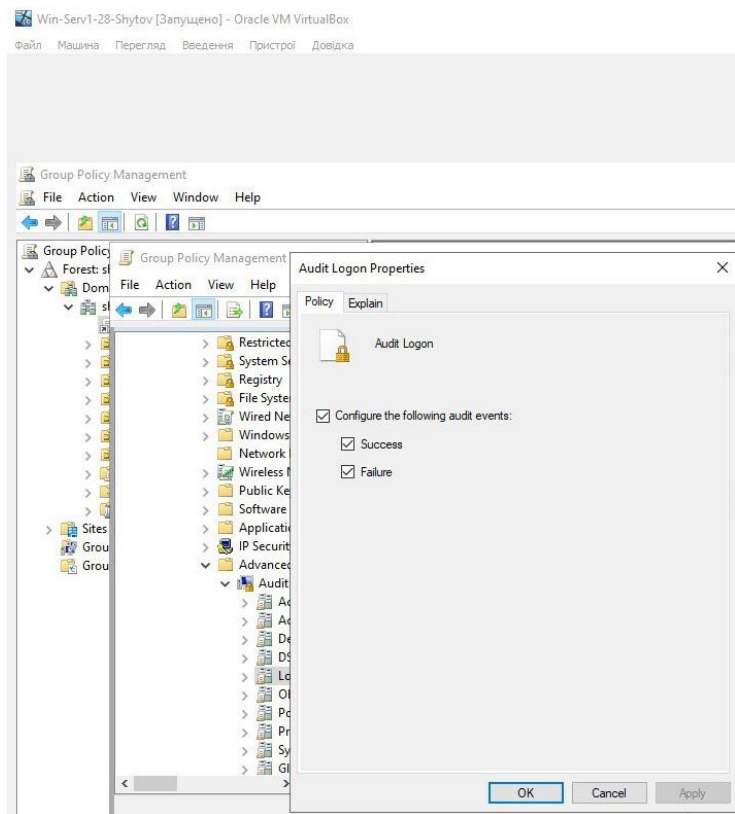


Рис. 3.1.30 Audit Logon Properties

Після проведених налаштувань ми можемо відслідковувати успішні або неуспішні події входу, виходу та підозрілі дії.

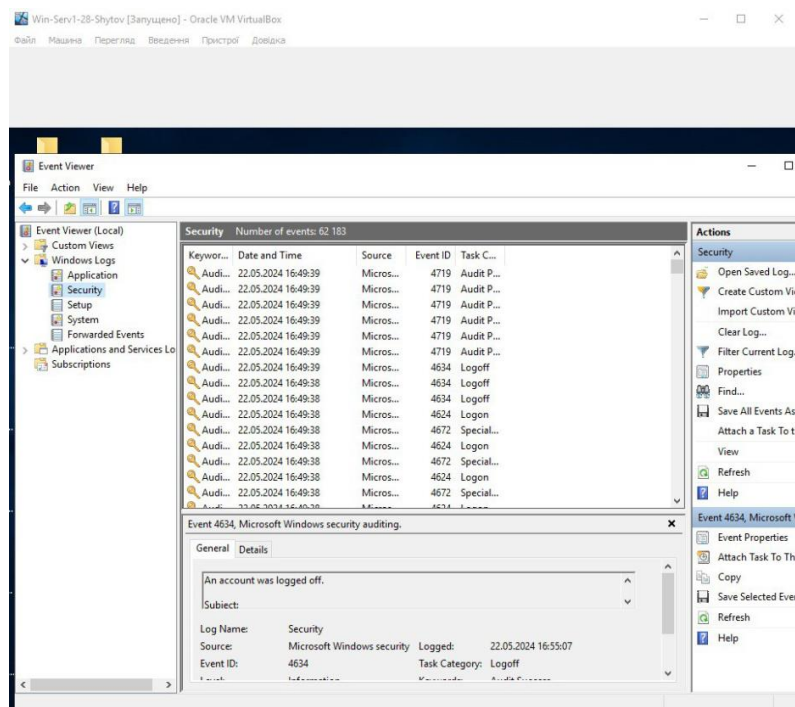


Рис. 3.1.31 Гілка Security у Event Viewer

На зображенні показано екран програми "Переглядач подій" (Event Viewer). У вікні відображаються журнали подій локальної машини.

Ліва частина вікна містить дерево навігації, де вибрано розділ "Windows Logs" -> "Security" (Журнали Windows -> Безпека).

Середня частина вікна показує список подій, зареєстрованих у журналі безпеки. Події відображаються з різними рівнями, джерелами та ідентифікаторами подій. Виділено подію з ідентифікатором 4634 від джерела "Microsoft Windows security auditing," що сталася 22.05.2024 о 16:55:07.

Нижня частина вікна показує деталі виділеної події. Опис події говорить: "An account was logged off" (Користувач вийшов з облікового запису).

Додаткові відомості включають:

- Log Name: Security (Журнал: Безпека)

- Source: Microsoft Windows security auditing (Джерело: Microsoft Windows аудит безпеки)
- Event ID: 4634 (Ідентифікатор події: 4634)
- Task Category: Logoff (Категорія завдання: Вихід з системи)
- Level: Information (Рівень: Інформація)
- Logged: 22.05.2024 16:55:07 (Зареєстровано: 22.05.2024 16:55:07)

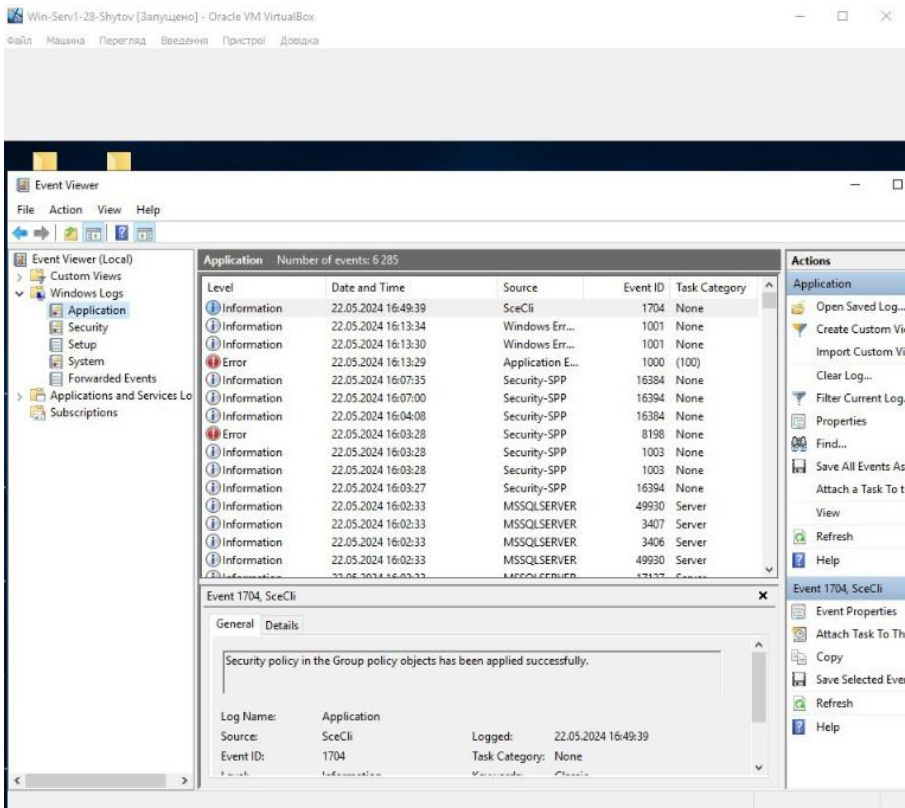


Рис. 3.1.32 Гілка Application у Event Viewer

На зображенні показано екран програми "Переглядач подій" (Event Viewer. У вікні відображаються журнали подій локальної машини.

Ліва частина вікна містить дерево навігації, де вибрано розділ "Windows Logs" -> "Application" (Журнали Windows -> Додаток).

Середня частина вікна показує список подій, зареєстрованих у журналі додатків. Виділено подію з джерела "SceCli" з ідентифікатором події 1704, яка сталася 22.05.2024 о 16:49:39.

Нижня частина вікна показує деталі виділеної події. Опис події говорить: "Security policy in the Group policy objects has been applied successfully." (Політика безпеки в об'єктах групової політики успішно застосована).

Додаткові відомості включають:

- Log Name: Application (Журнал: Додаток)
- Source: SceCli (Джерело: SceCli)
- Event ID: 1704 (Ідентифікатор події: 1704)
- Task Category: None (Категорія завдання: Немає)
- Level: Information (Рівень: Інформація)
- Logged: 22.05.2024 16:49:39 (Зареєстровано: 22.05.2024 16:49:39)

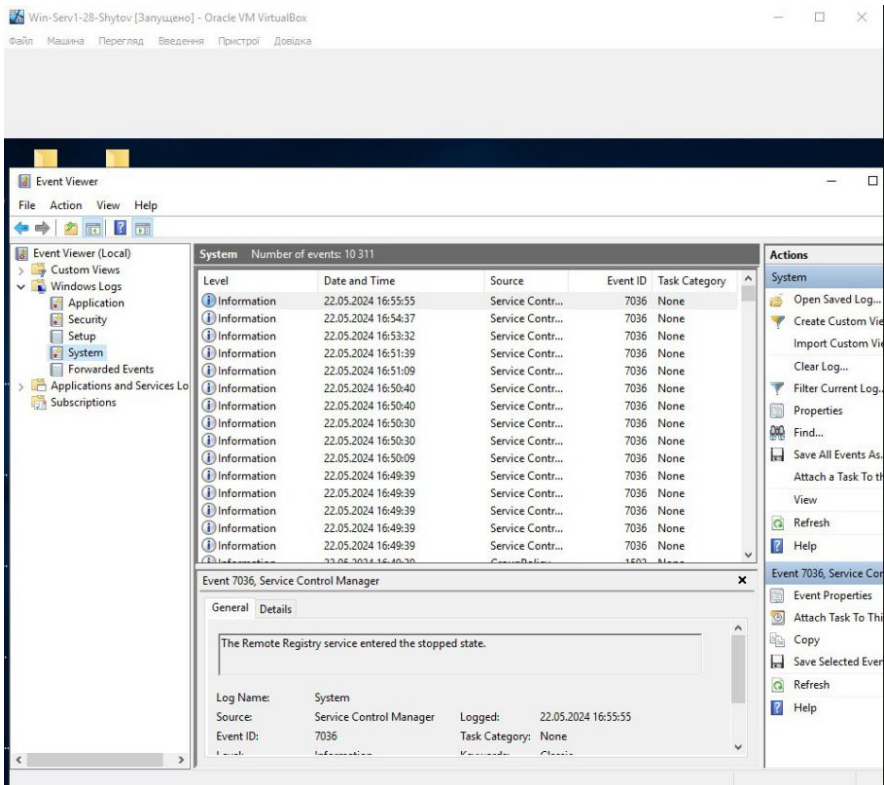


Рис. 3.1.33 Гілка System у Event Viewer

На зображенні показано екран програми "Переглядач подій" (Event Viewer). У вікні відображаються журнали подій локальної машини.

Ліва частина вікна містить дерево навігації, де вибрано розділ "Windows Logs" -> "System" (Журнали Windows -> Система).

Середня частина вікна показує список подій, зареєстрованих у системному журналі. Події відображаються з різними рівнями, джерелами та ідентифікаторами подій. Виділено подію з ідентифікатором 7036 від джерела "Service Control Manager," що сталася 22.05.2024 о 16:55:55.

Нижня частина вікна показує деталі виділеної події. Опис події говорить: "The Remote Registry service entered the stopped state." (Служба віддаленого реєстру перейшла у стан зупинки).

Додаткові відомості включають:

- Log Name: System (Журнал: Система)
- Source: Service Control Manager (Джерело: Диспетчер керування службами)
- Event ID: 7036 (Ідентифікатор події: 7036)
- Task Category: None (Категорія завдання: Немає)
- Level: Information (Рівень: Інформація)
- Logged: 22.05.2024 16:55:55 (Зареєстровано: 22.05.2024 16:55:55)

Також присутня можливість фільтрації подій за рівнем, часом, категорією, ключовими словами або користувачами:

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		62

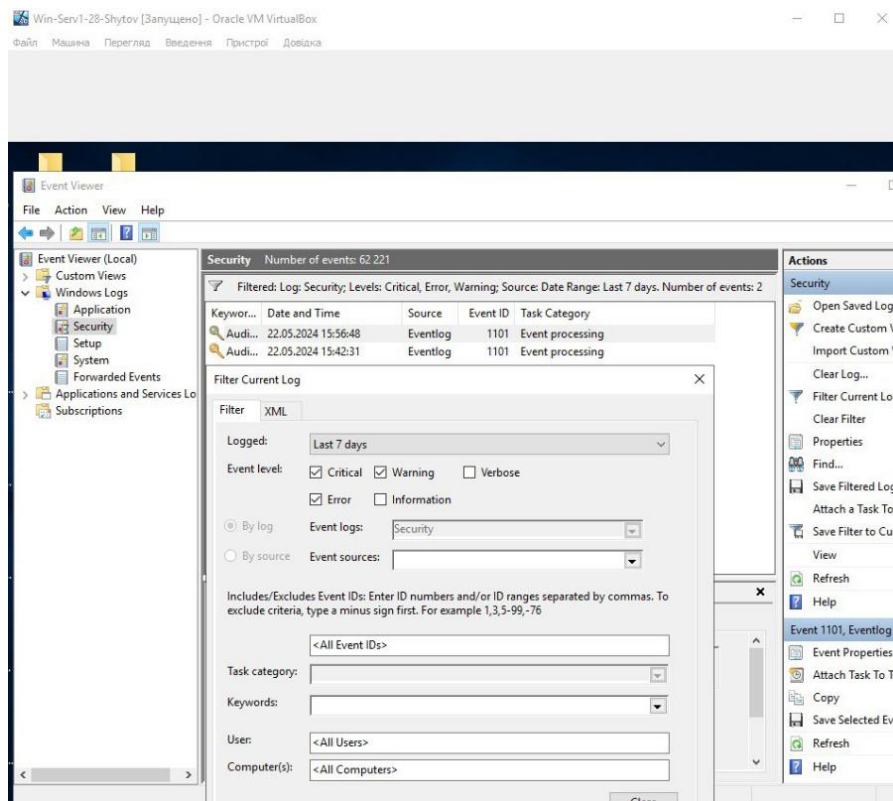


Рис. 3.1.34 Фільтрація подій у Event Viewer

Такі самі маніпуляції можна проводити за допомогою терміналу PowerShell, він є дуже зручним та швидим засобом відслідковування активності.

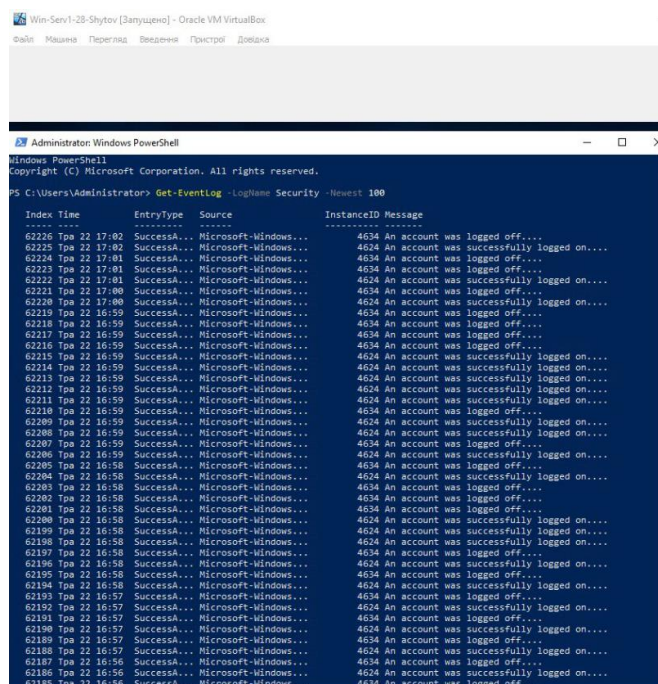


Рис. 3.1.35 Відслідковування подій Security за новизною (останні 100)

		Шитов Є.А			Арк.
		Фальковський І.Г			ККІКБ.КР.Б – 123 – 20 – ПЗ
Змн.	Арк.	№ докум.	Підпис	Дата	63

Створення та використання облікового запису керованої служби (MSA)

Налаштуємо обліковий запис керованої служби (MSA) для базового сайту IIS. Це допоможе забезпечити безпеку та автоматичне управління паролями для цієї служби.

Почнемо з встановлення MSA. Використаємо термінал PowerShell для швидкого та зручного встановлення MSA:

Команда `Import-Module ActiveDirectory` завантажує командлети Active Directory у середовище PowerShell, що дозволяє виконувати адміністративні завдання, такі як створення, видалення та оновлення облікових записів, управління групами і політиками безпеки в домені Active Directory.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Import-Module ActiveDirectory
```

Рис. 3.1.38 Import-Module ActiveDirectory

На зображенні показано вікно консолі Windows PowerShell, де виконуються команди для створення та додавання облікового запису служби (Service Account) в Active Directory:

```
PS C:\Users\Administrator> New-ADServiceAccount -Name EvgeniyMSA -RestrictToSingleComputer
PS C:\Users\Administrator> Add-ADComputerServiceAccount -Identity WIN-M0U00E0LQA2 -ServiceAccount EvgeniyMSA
PS C:\Users\Administrator>
```

Рис. 3.1.39 Створення та додавання облікового запису служби

`New-ADServiceAccount -Name EvgeniyMSA -RestrictToSingleComputer:` Команда для створення нового облікового запису служби з ім'ям "EvgeniyMSA", обмеженого для використання на одному комп'ютері.

`Add-ADComputerServiceAccount -Identity WIN-M0U00E0LQA2 -ServiceAccount EvgeniyMSA:` Команда для додавання облікового запису служби "EvgeniyMSA" до комп'ютера з ідентифікатором "WIN-M0U00E0LQA2".

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		65

Далі виконуємо команди для встановлення та перевірки керованого облікового запису служби (Managed Service Account, MSA) в Active Directory:

```
PS C:\Users\Administrator> Install-ADServiceAccount -Identity EvgeniyMSA
PS C:\Users\Administrator> Test-ADServiceAccount -Identity EvgeniyMSA
True
PS C:\Users\Administrator>
```

Рис. 3.1.40 Перевірка встановлення MSA

Результат True свідчить про успішне встановлення служби.

Далі перейдемо до безпосереднього використання служби MSA. Спочатку налаштуємо квоти пам'яті для процесу (Adjust memory quotas for a process). Це налаштування дозволяє адміністратору визначити квоти пам'яті для процесу для певних користувачів або облікових записів служб. У даному випадку, обліковий запис служби "EvgeniyMSA" додається до списку об'єктів, на які будуть застосовані ці квоти пам'яті. Це забезпечує контроль над тим, скільки пам'яті може використовувати певний процес, пов'язаний з цим обліковим записом служби.

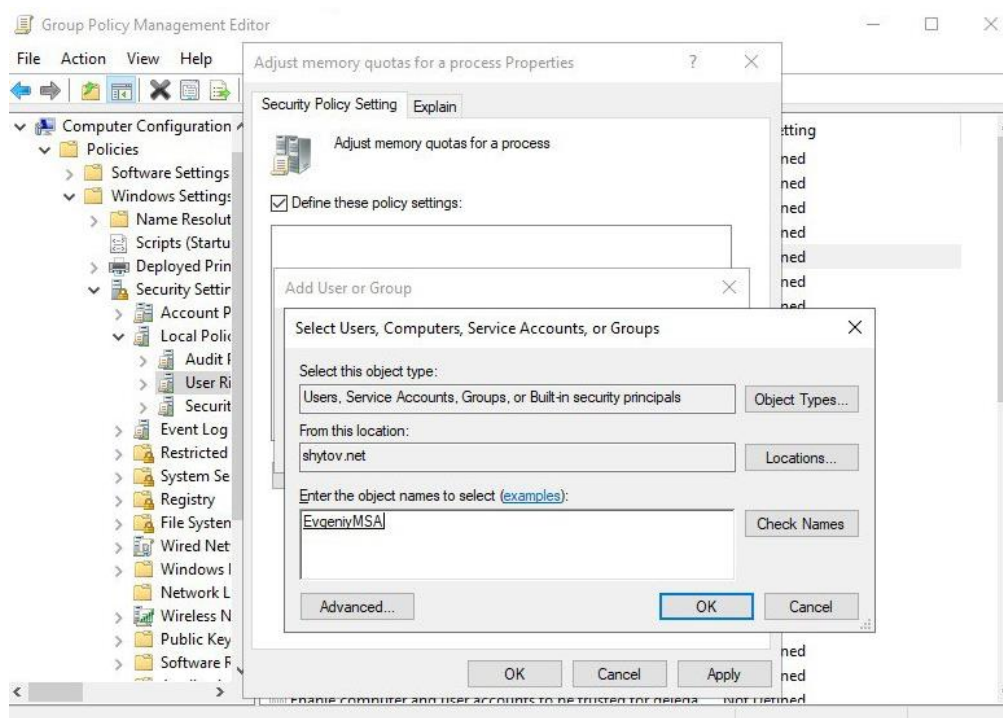


Рис. 3.1.41 Adjust memory quotas for a process

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				66
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі налаштуємо заміну токена рівня процесу (Replace a process level token). Ця привілея дозволяє програмам або службам замінювати токен рівня процесу, що може бути необхідно для виконання певних адміністративних завдань або для зміни контексту безпеки процесу.

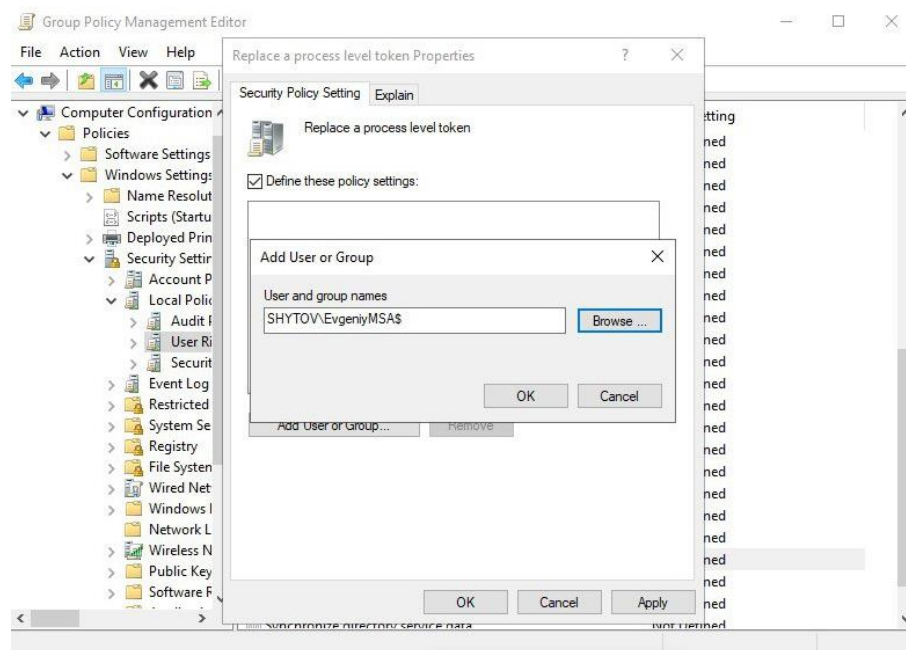


Рис. 3.1.42 Replace a process level token

Примусово оновлюємо політики:

```
PS C:\Users\Administrator> gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

Рис. 3.1.43 Примусове оновлення політик

Переходимо до використання готового аккаунта MSA для базового сайту DefaultAppPool:

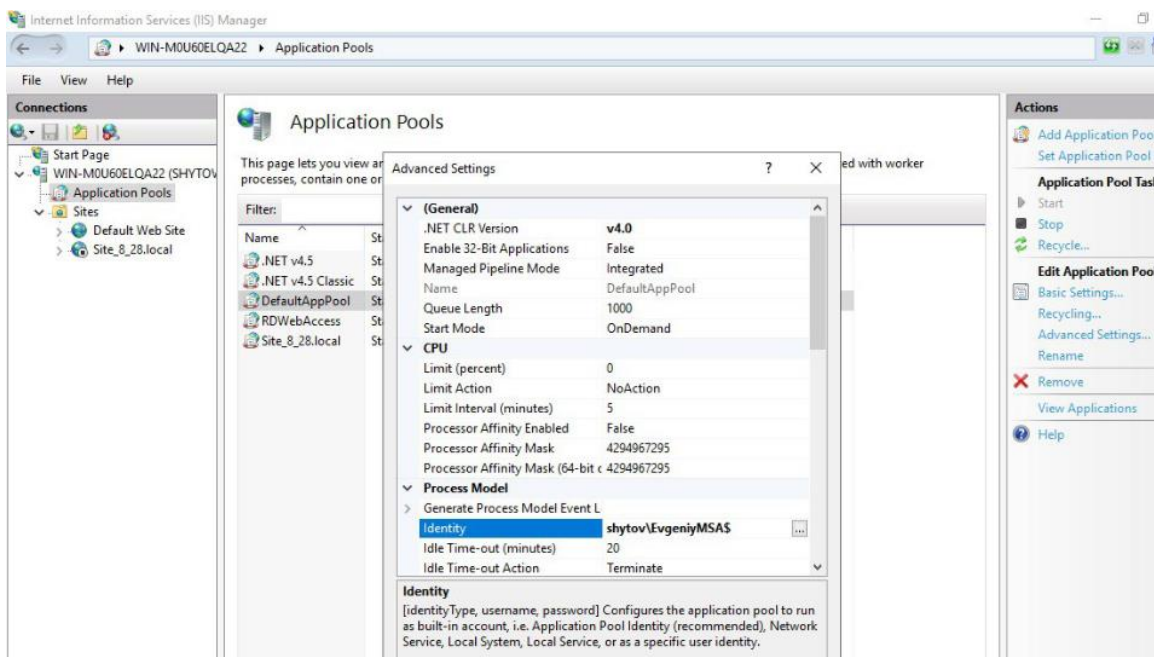


Рис. 3.1.44 менеджера служб Інтернету (Internet Information Services, IIS)

Цей екран показує, як налаштовуються пули додатків в IIS, включаючи використання керованого облікового запису служби (Managed Service Account, MSA) для пулу додатків. У цьому випадку, обліковий запис служби "EvgeniyMSA" використовується для забезпечення безпеки та ізоляції процесів, що виконуються в цьому пулі додатків.

Щоб вхід з аккаунта MSA відобразився у Event Viewer нам потрібно запустити сайт і здійснити там будь-яку активність:

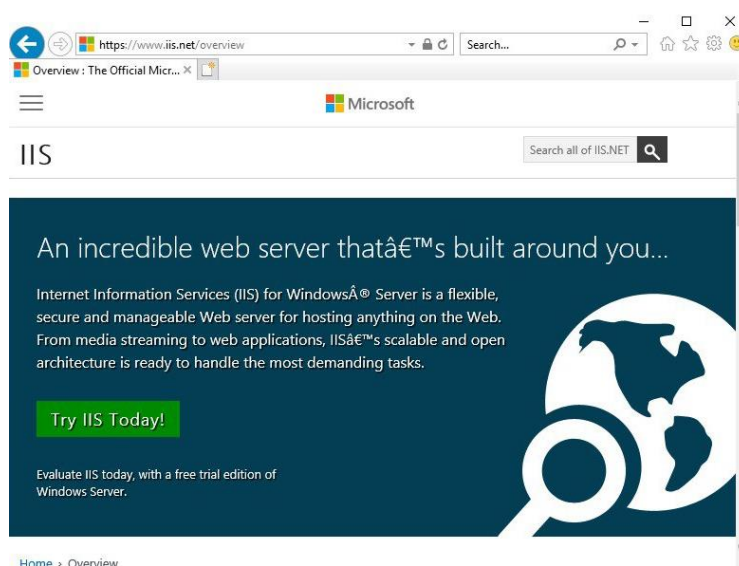


Рис. 3.1.45 Здійснення активності на сайті

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		68

Після цього у Event Viewer ми можемо спостерігати лог з даними входу з аккаунту MSA:

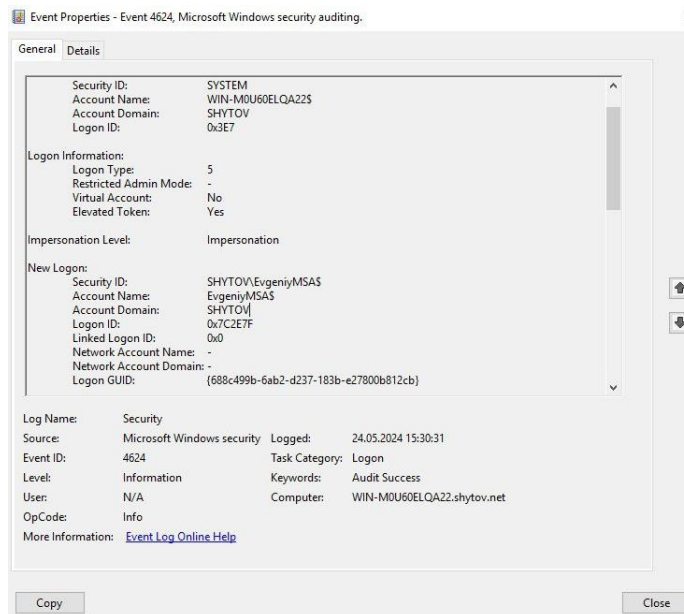


Рис. 3.1.46 Лог з успішним входом в аккаунт

На зображенні показано вікно властивостей події (Event Properties) з журналу безпеки Windows, яке відображає деталі події з ідентифікатором 4624. Ця подія стосується успішного входу в систему (Logon). Ця подія свідчить про успішний вхід у систему за допомогою облікового запису служби "EvgeniyMSA".

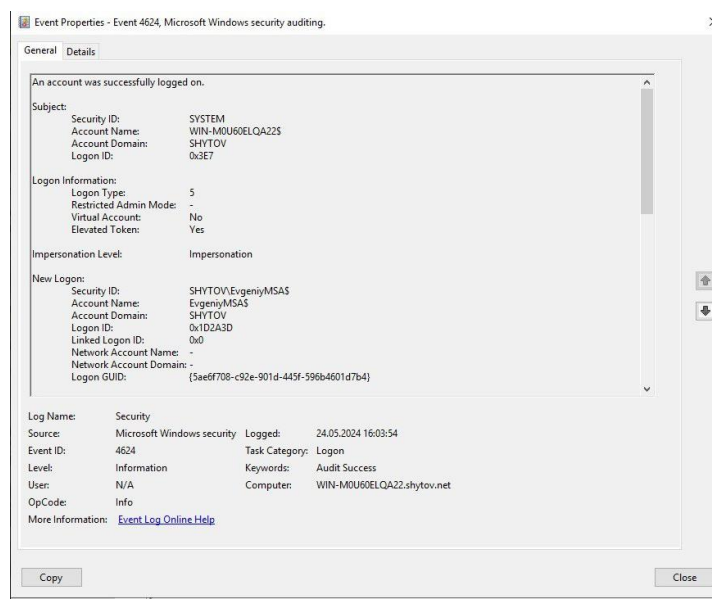


Рис. 3.1.47 Лог з успішним входом в аккаунт

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				69
Змн.	Арк.	№ докум.	Підпис	Дата		

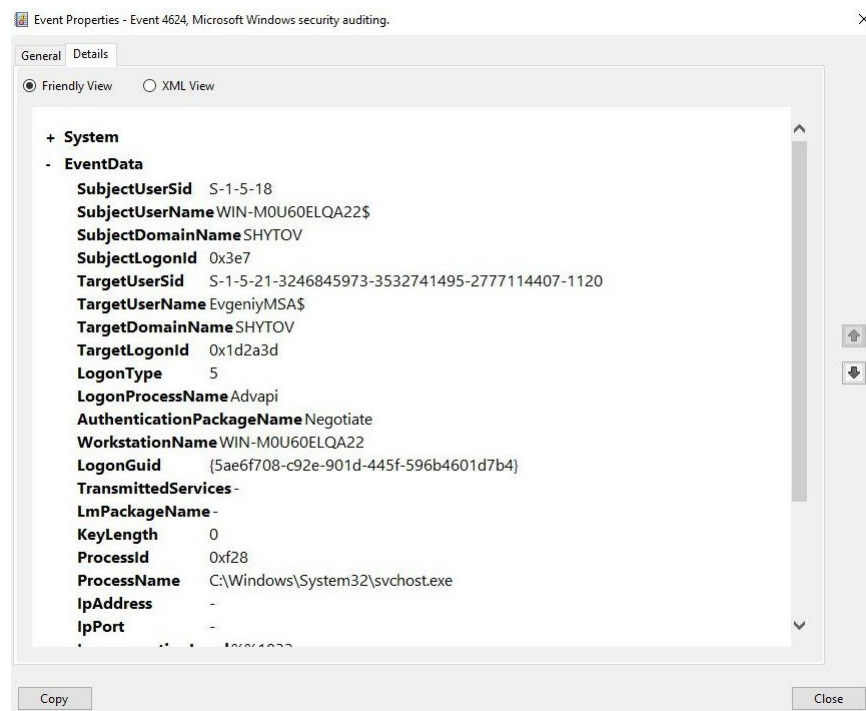


Рис. 3.1.48 Більш детальна інформація з логу з успішним входом в
акаунт MSA

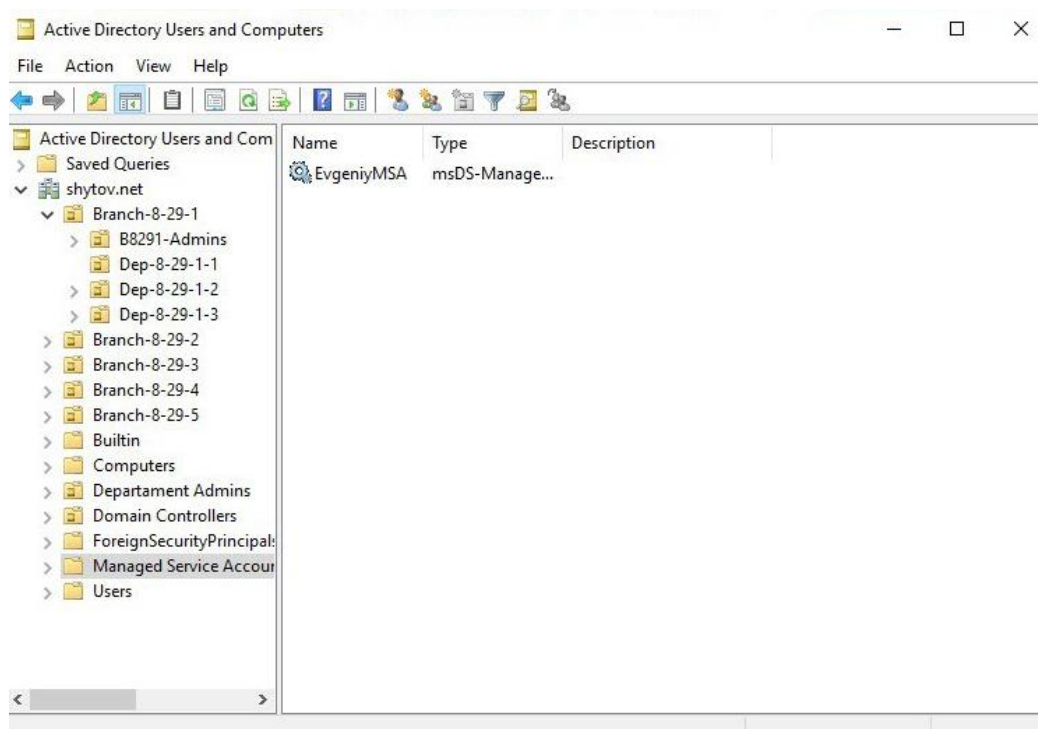


Рис. 3.1.49 Відображення готового Managed Service Account

		Шитов С.А.			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Встановлення та налаштування двофакторної аутентифікації від Rublon.

Двофакторна аутентифікація — це процес підтвердження ідентичності користувача за допомогою двох різних методів аутентифікації. Зазвичай це включає в себе щось, що користувач знає (наприклад, пароль) і щось, що користувач має (наприклад, мобільний пристрій, на який надсилається SMS-код або генерується токен).

Почнемо з встановлення аутентифікатора на контролері домену і робочій станції:



Рис. 3.2.1 Встановлення Rublon серверу

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				71
Змн.	Арк.	№ докум.	Підпис	Дата		

Вписуємо системний токен та ключ для підв'язки кабінету для входу:

Setup - Rublon for Windows Logon and RDP

Set up credentials
Enter System Token and Secret Key values

System Token:
071365AD2E7C49BF939A784F55F4B1F9

Secret Key:
874ae74b0b7a311200dabeaf5ccc3c

☒ Show key

Enter API credentials for the application created in the [Rublon Admin Console](#).

If you do not have any application of type "Windows Logon and RDP", you must create one in the Applications tab.
Correct System Token and Secret Key parameters are required to proceed further.

Rublon Documentation Back Next Cancel

Рис. 3.2.2 Встановлення токена та ключа

Далі обираємо потрібні пункти які відповідають нашим вимогам:

Setup - Rublon for Windows Logon and RDP

Configuration
These settings allow you to change the default behavior of Rublon in certain scenarios

☐ Prompt for MFA only for RDP logins

☐ Enable User Account Control (UAC) elevation protection

☐ Use proxy

Prompt for MFA only for RDP logins
Check to make only RDP sessions prompt for MFA. Local Windows logins will be bypassed.

Enable User Account Control (UAC) elevation protection
Check to make Rublon challenge non-admin users for MFA every time the UAC elevation prompt appears.

Use proxy
Check to enable proxy. You will be able to provide proxy information on the next page of this setup wizard.

Rublon Documentation Back Next Cancel

Рис. 3.2.3 Обираємо необхідні нам пункти

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		72

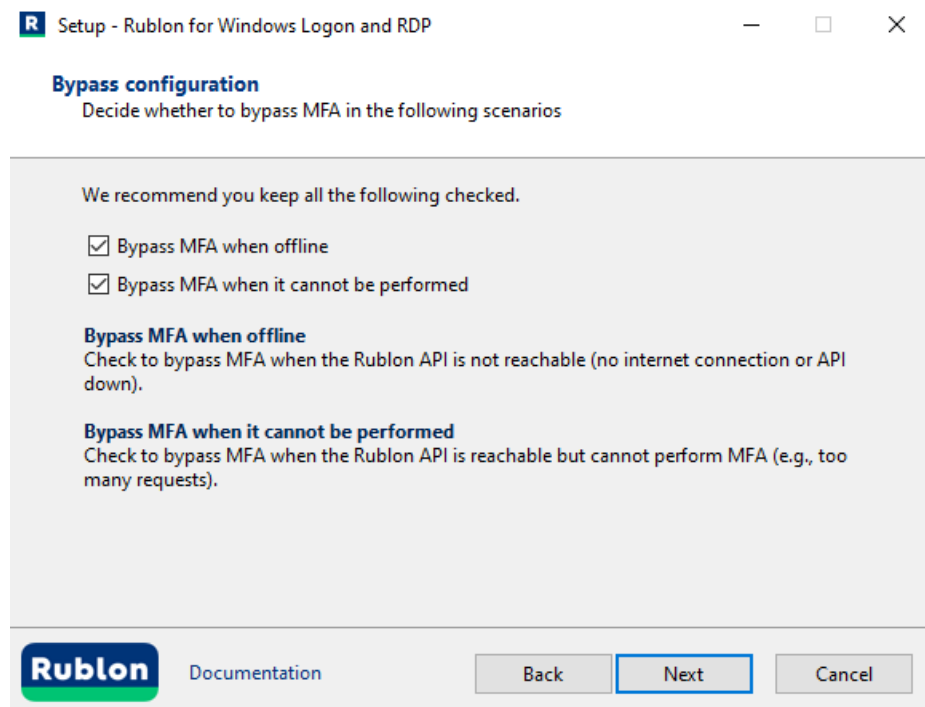


Рис. 3.2.4 Обираємо необхідні нам пункти

Далі налаштовуємо підключення до телефону користувача:

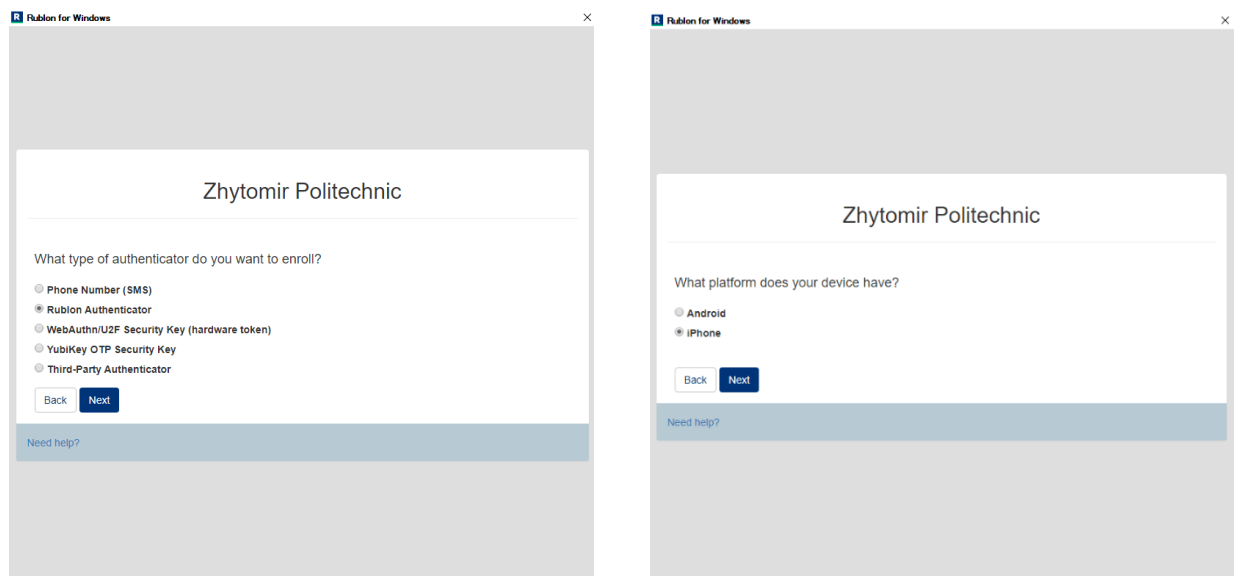


Рис. 3.2.5-6 Обираємо тип аутентифікації

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		73

Кінцеве підтвердження і тест налаштованого аутентифікатора:

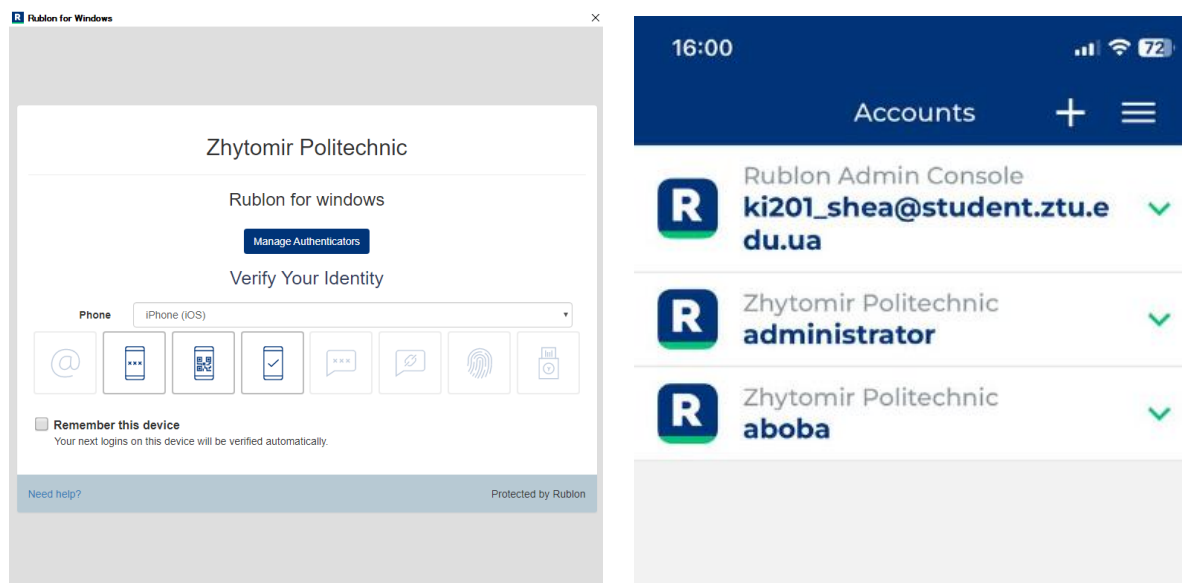


Рис. 3.2.7-8 Додані аккаунти у мобільному додатку

Після проведення налаштувань Rublon на Windows сервер, користувач почне отримувати мобільні повідомлення при спробі аутентифікації в робочих станціях чи доменних контролерах. Також користувачі отримують свої електронні кабінети за допомогою яких можна відслідковувати входи на певні пристрої:

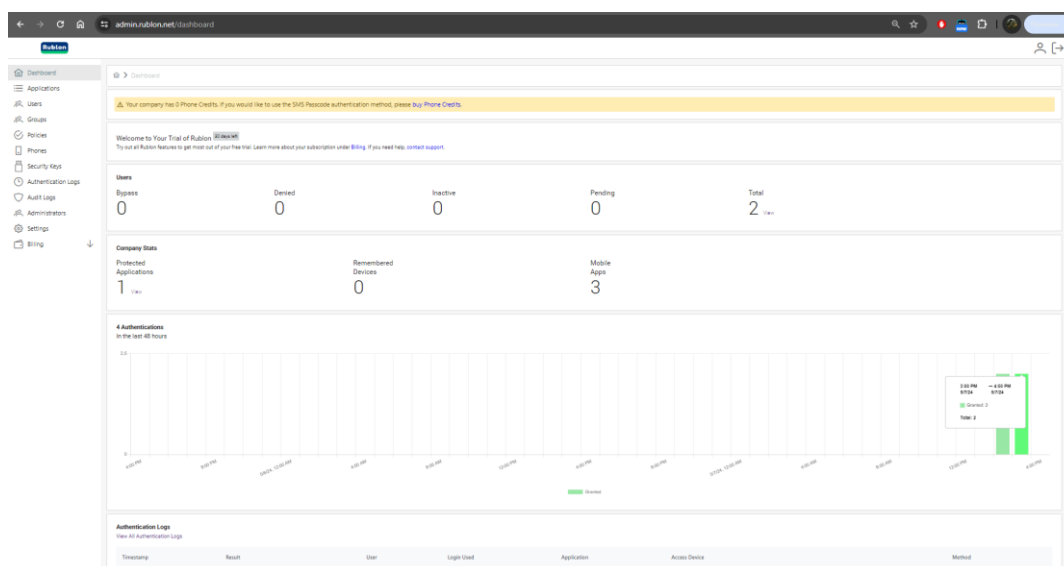


Рис. 3.2.9 Головна сторінка адміністратора

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		74

Адміністратор може додавати або вилучати користувачів для двофакторної аутентифікації:

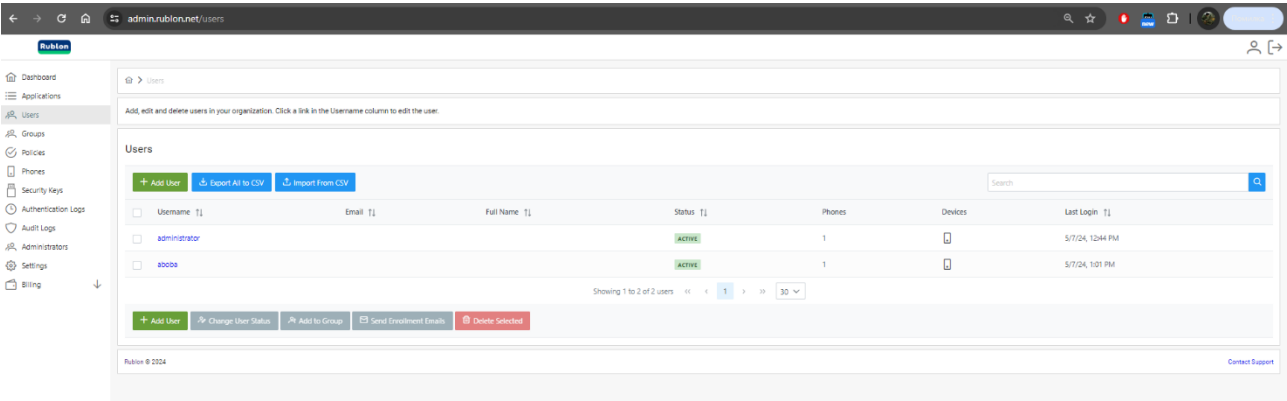


Рис. 3.2.10 Сторінка Юзерів

Також можна відслідковувати пристрої які користувачі прив’язали до своїх аутентифікаторів:

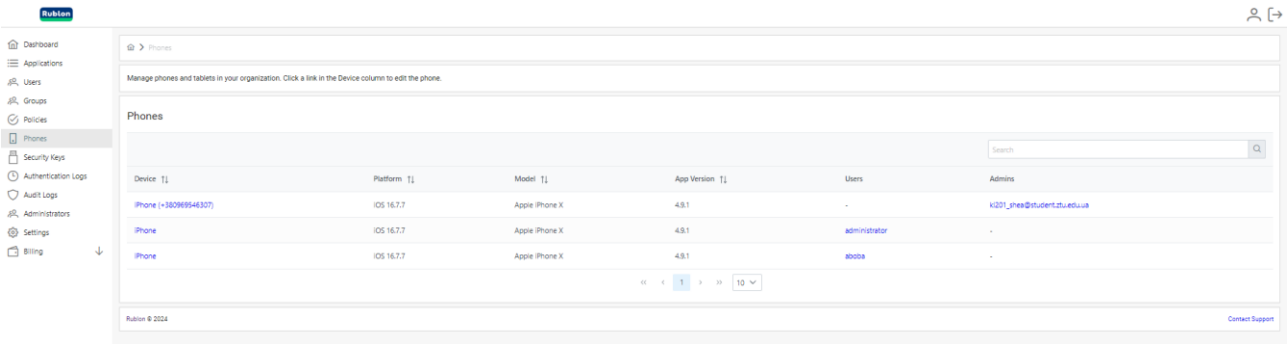
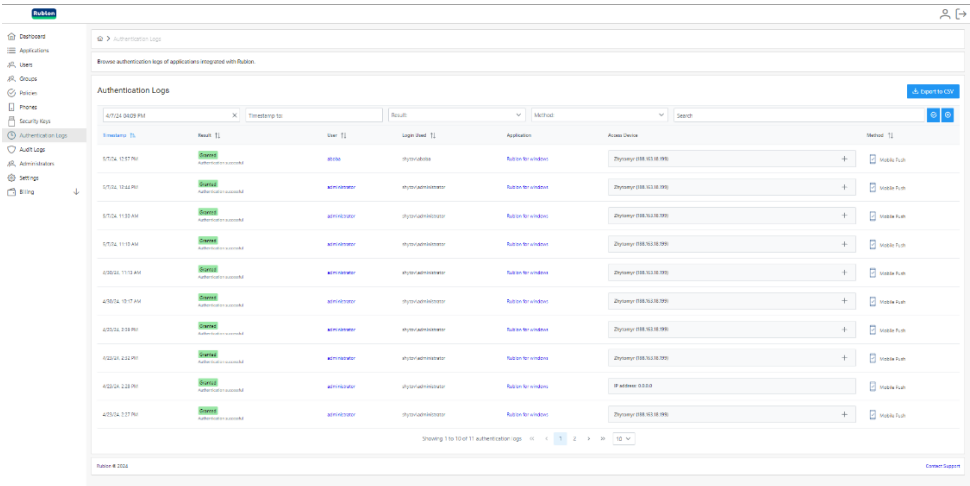


Рис. 3.2.11 Прив’язані пристрої користувачів

Основним плюсом аутентифікатору від Rublon – це легке відслідковування логів та аудитів входу,що дає змогу захистити контролери та пристрої від небажаного втручання.



Audit Logs

Review audit logs to track administrator activities in your organization. Click a link in the Activity column for detailed information.

Timestamp: 04/07/2024 04:10 PM | Search

Timestamp	Location	Actor	Activity
5/1/24, 1:05 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
5/1/24, 1:03 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
5/1/24, 12:47 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
5/1/24, 11:52 AM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
4/23/24, 3:01 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
4/23/24, 2:38 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In
4/23/24, 2:37 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Updated Administrator k201_uhes@student.ru.edu.ua (Owner)
4/23/24, 1:47 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Created Application Rubicon for windows (Windows Logon & RDP)
4/23/24, 1:46 PM	Zhytomyr 188.165.18.159	Egermyr Shytlov k201_uhes@student.ru.edu.ua	Successful Sign-In

Showing 1 to 9 of 9 audit logs | Page 1 of 1

Рис. 3.2.12-13 Аудити входів на пристрої



Рис. 3.2.14 Вигляд підтвердження в телефоні користувача

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковский І.Г				76
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Налаштування NAT

Налаштування NAT

У наш час кожна мережа має мати можливість у виходу у Інтернет, тому є необхідність у налаштуванні зв'язку, для цього буде використано NAT Overload.

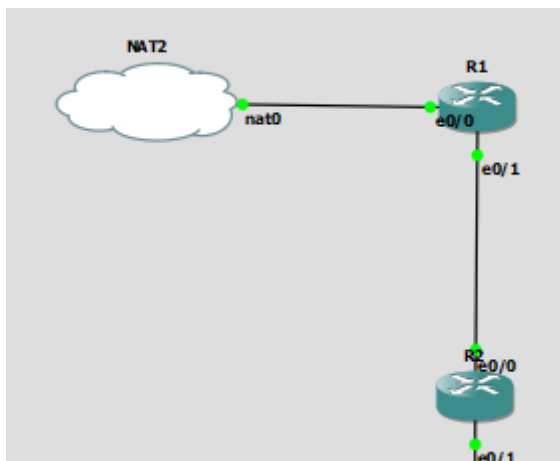


Рис. 3.3.1 Налаштування NAT

Для реалізації налаштувань було використано 2 маршрутизатори Cisco і були введені такі налаштування:

R1

```
conf t
int e0/0
ip nat outside
exit
int e0/1
ip nat inside
exit
ip nat inside source list 1 interface e0/0 overload
access-list 1 permit any
int e0/0
ip address dhcp
no sh
int e0/1
ip address 10.1.1.254 255.255.255.0
no sh
ex
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
default-information originate
end
```

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				77
Змн.	Арк.	№ докум.	Підпис	Дата		

R2

```
conf t
int e0/0
ip address 10.1.1.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 10.1.1.254
ip domain-lookup
ip name-server 8.8.8.8 8.8.4.4
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
network 214.8.29.0 0.0.0.31 area 0
default-information originate
end
```

Після проведення відповідних налаштувань мережа має вихід у Інтернет.

Отже аутентифікація буде відбуватись успішно.

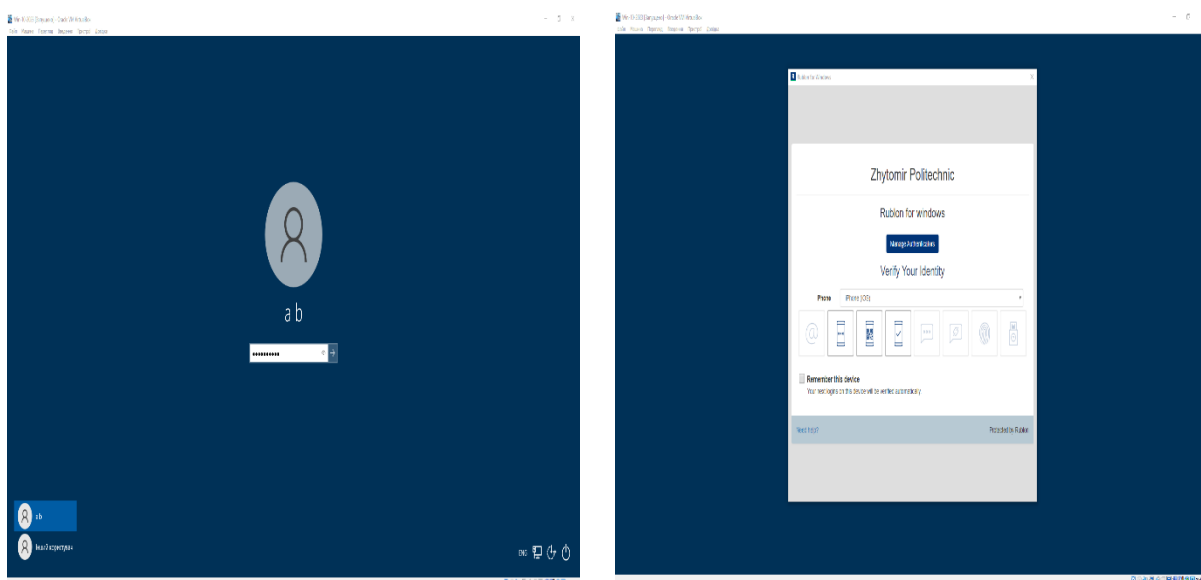


Рис. 3.3.2-3 Успішна робота Інтернету для аутентифікації

3.4 Відновлення після інцидентів

Резервне копіювання (бекап) по розкладу на доменному контролері Windows Server 2019 має критичне значення для забезпечення безперервної роботи та захисту даних в організаціях.

Спочатку потрібно встановити функцію резервного копіювання:

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		78

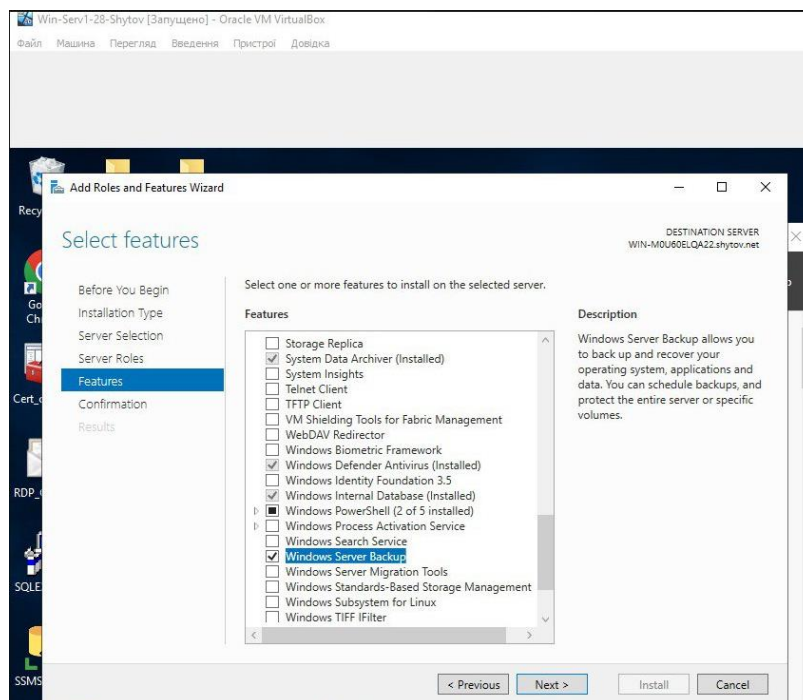


Рис. 3.4.1 Вибір функції резервного копіювання

Після цього переходимо безпосередньо до встановлення:

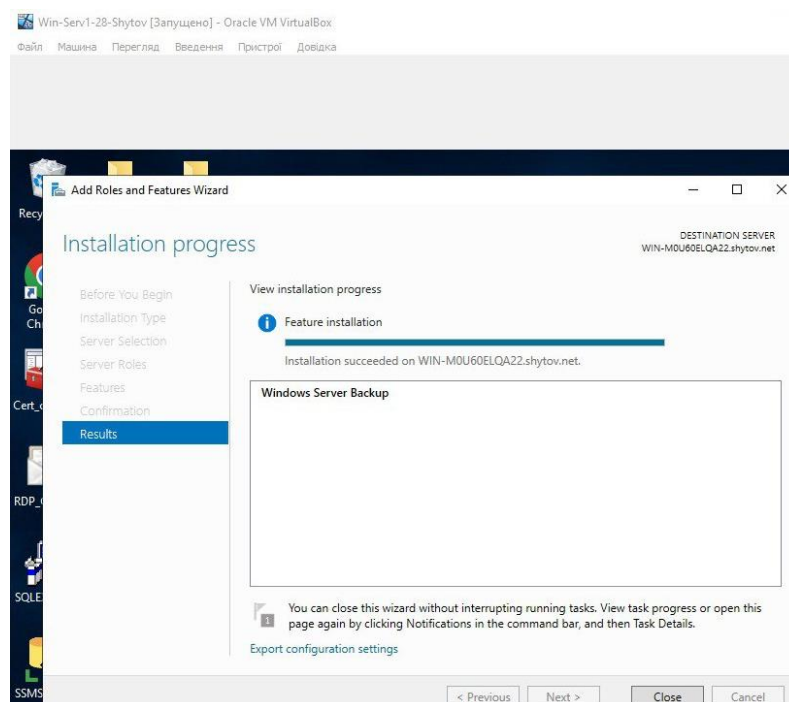


Рис. 3.4.2 Успішне встановлення резервного копіювання

Після встановлення переходимо до інтерфейсу програми Windows Server Backup.

		Шитов С.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				79
Змн.	Арк.	№ докум.	Підпис	Дата		

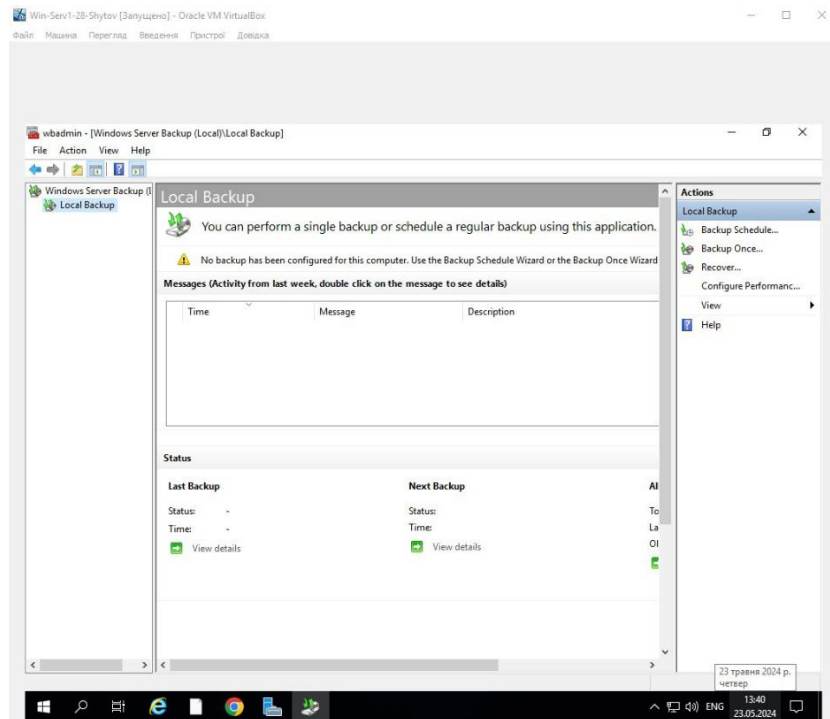


Рис. 3.4.3 Інтерфейс Windows Server Backup

У рамках данної роботи потрібно зосередити увагу саме на правій секції програми.

Права частина вікна (панель дій):

- Actions (Дії):
- Local Backup (Локальне резервне копіювання): Активний розділ.
- Backup Schedule (Розклад резервного копіювання): Налаштування розкладу регулярного резервного копіювання.
- Backup Once (Одноразове резервне копіювання): Запуск одноразового резервного копіювання.
- Recover (Відновлення): Відновлення даних з резервної копії.
- Configure Performance Settings (Налаштування продуктивності): Налаштування параметрів продуктивності резервного копіювання.

Обираємо пункт Backup Schedule та переходимо до налаштування:

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				80
Змн.	Арк.	№ докум.	Підпис	Дата		

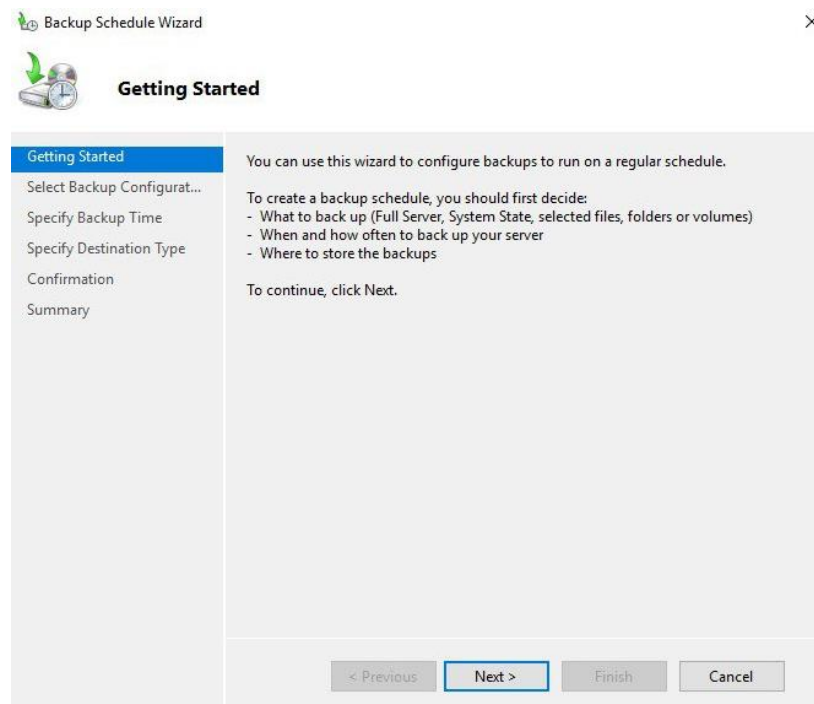


Рис. 3.4.4 Інтерфейс Backup Schedule Wizard

Обираємо тип резервного копіювання. В данному випадку – за замовчуванням:

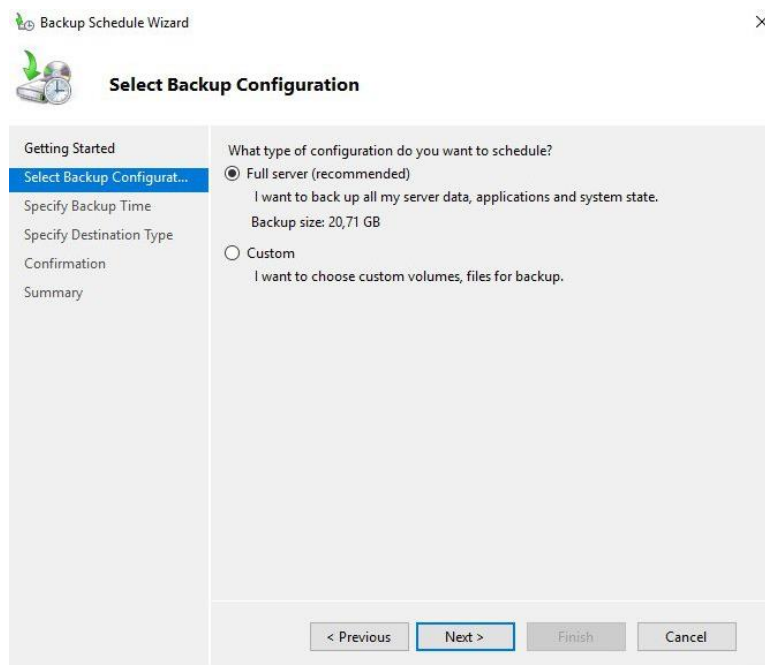


Рис. 3.4.5 Backup Schedule Wizard

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				81
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі потрібно обрати частоту резервного копіювання та час у який воно буде проводитись:

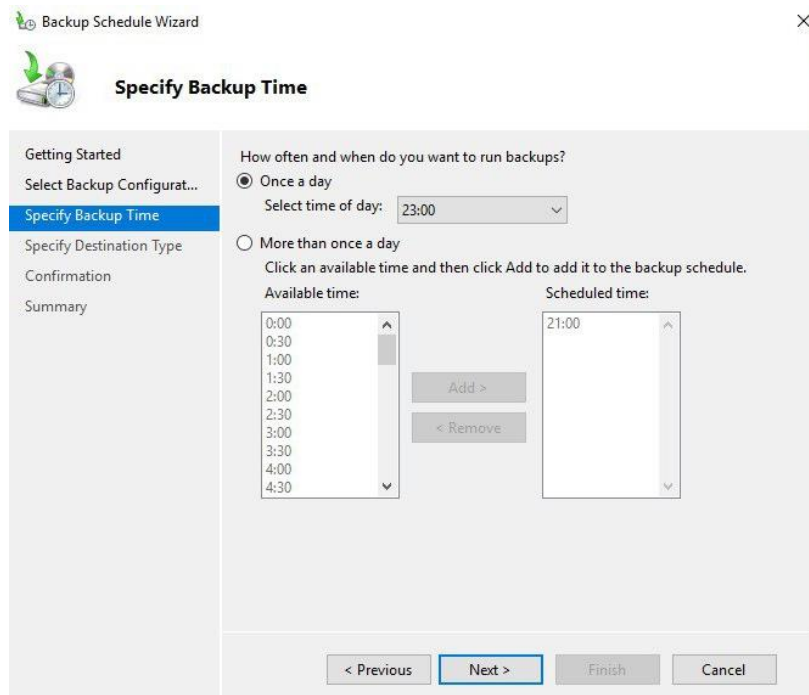


Рис. 3.4.6 Встановлення розкладу копіювання

Після цього потрібно обрати місце куди будуть записуватись резервні копії даних:

- Back up to a hard disk that is dedicated for backups (Резервне копіювання на жорсткий диск, призначений для резервних копій).
- Back up to a volume (Резервне копіювання на тому)
- Back up to a shared network folder (Резервне копіювання в спільну мережеву папку)

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				82
Змн.	Арк.	№ докум.	Підпис	Дата		

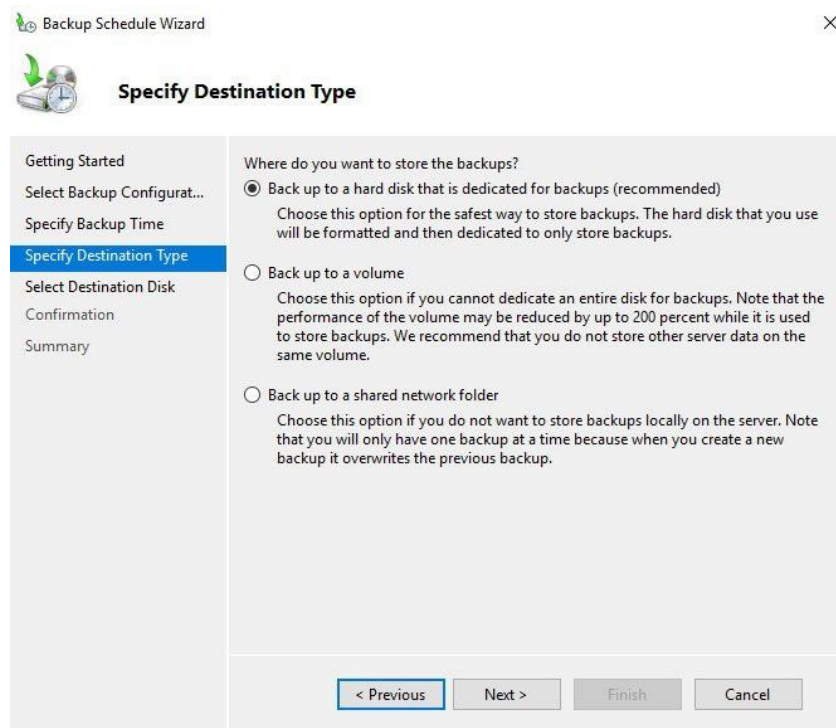


Рис. 3.4.7 Вибір місця для резервного копіювання

Так як був обраний варіант (Резервне копіювання на жорсткий диск, призначений для резервних копій) обираємо потрібний жорсткий диск:

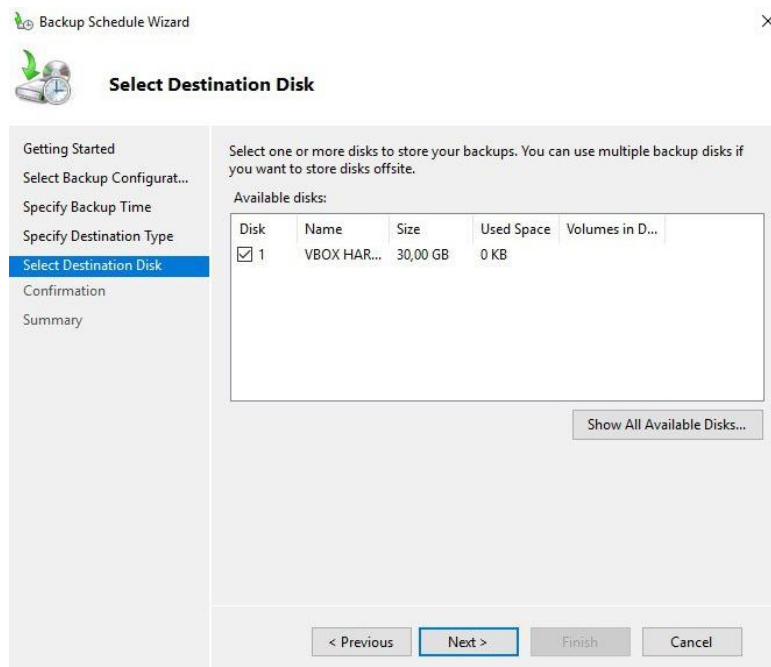


Рис. 3.4.8 Вибір місця для резервного копіювання

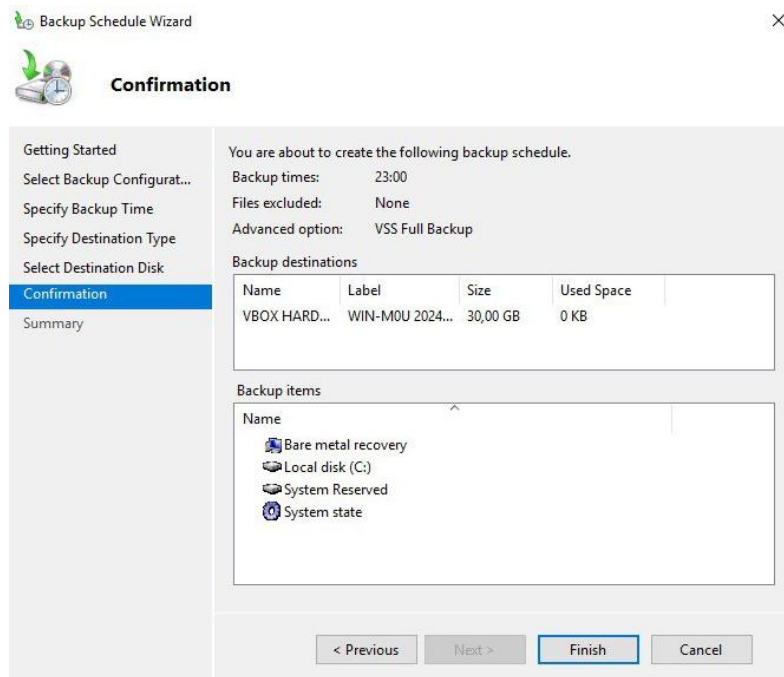


Рис. 3.4.9 Вибір місця для резервного копіювання

У розділі Summary можна спостерігати що резервне копіювання буде проводитись кожен день о 23:00.

Підтверджуємо і завершуємо налаштування:

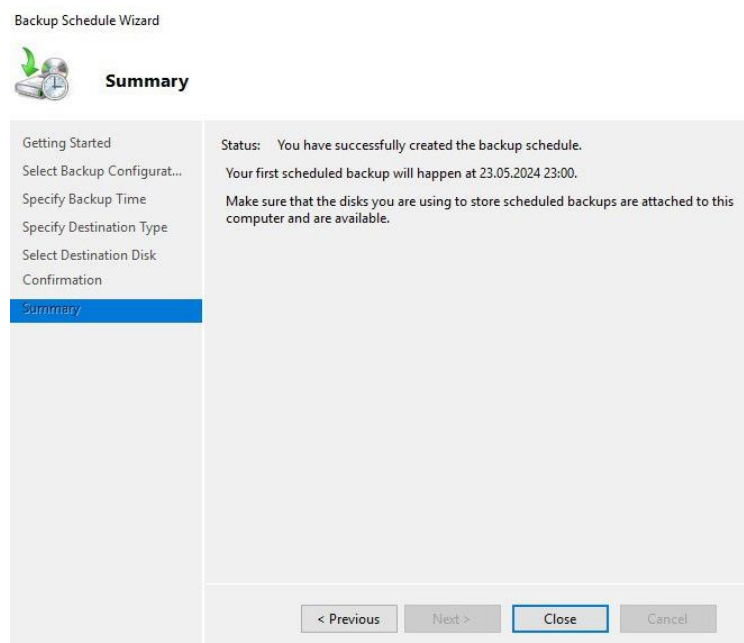


Рис. 3.4.10 Завершення налаштування

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		84

Тепер у програмі Windows Server Backup можна спостерігати заплановане резервне копіювання:

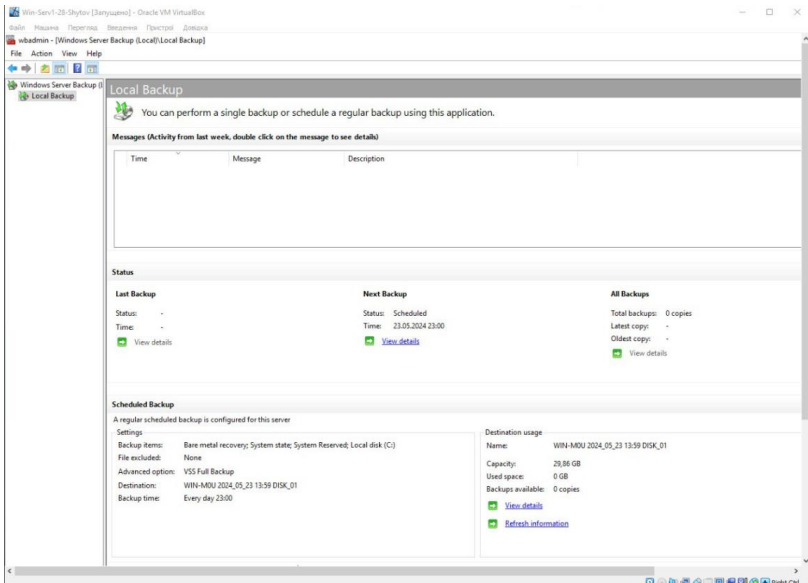


Рис. 3.4.11 Фінальний вигляд Windows Server Backup після налаштування

Висновки: У третьому розділі було детально описано процес встановлення та налаштування системи захисту мережі на основі Active Directory, зокрема процес встановлення та налаштування серверів Microsoft Active Directory. Цей розділ надає практичні кроки та рекомендації з реалізації засобів захисту на основі використання Active Directory. Розглянуто налаштування базових політик паролів, блокування облікових записів, детальних політик паролів, а також аудиту входу-виходу. Описано процес створення та налаштування облікових записів керованих служб (MSA) та налаштування резервного копіювання. Крім того, було розглянуто налаштування NAT для забезпечення коректного доступу до Інтернету.

ЗАГАЛЬНІ ВИСНОВКИ

У розділі 1 було проведено детальний огляд технології служби Active Directory, її загальний опис та можливості використання для побудови захищеної мережі. Виявлено, що Active Directory володіє широким спектром функцій, які дозволяють ефективно управляти користувачами, групами та ресурсами в мережі.

Розділ 2 присвячений проектуванню налаштувань захисту активних доменних контролерів на базі Active Directory та вибору засобів двофакторної аутентифікації. В результаті аналізу було розроблено оптимальну топологію комп'ютерної мережі, схему адресації мережі та вибрано найбільш підходящі засоби для забезпечення додаткового рівня безпеки за допомогою двофакторної аутентифікації.

У третьому розділі було детально описано процес встановлення та налаштування системи захисту мережі на основі Active Directory, зокрема процес встановлення та налаштування серверів Microsoft Active Directory. Цей розділ надає практичні кроки та рекомендації з реалізації засобів захисту на основі використання Active Directory. Розглянуто налаштування базових політик паролів, блокування облікових записів, детальних політик паролів, а також аудиту входу-виходу. Описано процес створення та налаштування облікових записів керованих служб (MSA) та налаштування резервного копіювання. Крім того, було розглянуто налаштування NAT для забезпечення коректного доступу до Інтернету.

Загальним висновком можна сказати, що використання Active Directory для побудови захищеної мережі є доцільним та ефективним підходом, який дозволяє забезпечити високий рівень безпеки та ефективного управління ресурсами мережі. Реалізація запропонованих у роботі заходів з захисту та налаштування системи на основі Active Directory сприятиме підвищенню загального рівня безпеки корпоративної мережі.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		86

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 101 of the Latest Data Breach Statistics for 2024 [Електроний ресурс] / secureframe.- <https://secureframe.com/blog/data-breach-statistics>
01.01.2024 – Загол. з екрану
2. Active Directory [Електроний ресурс] / Wikipedia .- https://uk.wikipedia.org/wiki/Active_Directory 05.02.2024 – Загол. з екрану
3. Kerberos Authentication Overview [Електроний ресурс] / Microsoft .- <https://learn.microsoft.com/ru-ru/windows-server/security/kerberos/kerberos-authentication-overview> - 25.08.2023 – Загол. з екрану
4. Securing Domain Controllers Against Attack [Електроний ресурс] / Microsoft .- <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack> - 05.30.2024 – Загол. з екрану
5. Active Directory Domain Services Overview [Електроний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> – 17.08.2022. – Загол. з екрану.
6. Kerberos Authentication Overview [Електроний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/ru-ru/windows-server/security/kerberos/kerberos-authentication-overview> – 21.12.2022. – Загол. з екрану.
7. Password Policy Microsoft [Електроний ресурс] / Microsoft. – <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-policy> – 04.19.2017. – Загол. з екрану
8. Account Lockout Policy Microsoft [Електроний ресурс] / Microsoft. – <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/account-lockout-policy>

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		87

- pro/windows-10/security/threat-protection/security-policy-settings/account-lockout-policy – 10.11.2018. – Загол. з екрану
9. Introduction to Active Directory Administrative Center Enhancements (Level 100) [Електроний ресурс] / Microsoft. – <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/introduction-to-active-directory-administrative-center-enhancements--level-100> – 07.29.2021. – Загол. з екрану
 10. Useful PowerShell commands for managing Active Directory password policies [Електроний ресурс] / specops. - <https://specopssoft.com/blog/managing-active-directory-password-policy-with-powershell/> - 07.08.2023. – Загол. з екрану
 11. Audit Policy Recommendations [Електроний ресурс] / Microsoft - <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations> - 08.04.2023. – Загол. з екрану
 12. Group Managed Service Accounts Overview [Електроний ресурс] / Microsoft. - <https://learn.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview> - 05.08.2023 – Загол. з екрану
 13. Incident Response Reference Guide [Електроний ресурс] / Microsoft guidebook. - <https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-emergency-doc-digital.pdf> - 01.01.2017 – Загол. з екрану
 14. Guidance for Incident Responders [Електроний ресурс] / Microsoft guidebook. - <https://cdndynmedia1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/IR-Guidebook-Final.pdf> - 01.01.2017 – Загол. з екрану
 15. Computer Security Incident Handling Guide [Електроний ресурс] / NISTguidebook. -

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				88
Змн.	Арк.	№ докум.	Підпис	Дата		

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
-01.01.2017 – Загол. з екрану

16. What Is Network Address Translation? [Електронний ресурс] / Microsoft Learn. – <https://www.comptia.org/content/guides/what-is-network-address-translation#:~:text=What%20Is%20NAT%3F,as%20do%20most%20home%20routers> – 17.08.2022. – Загол. з екрану.

17. Що таке двохфакторна автентифікація? [Електронний ресурс] / Microsoft.- <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-> 01.01.2024 – Загол. з екрану

18. Фішинг [Електронний ресурс] / ESET.- <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/fishing/> 01.01.2024 – Загол. з екрану

19. Атака Pass-the-hash [Електронний ресурс] / Wikipedia.- https://uk.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_Pass-the-hash -23.03.2024 – Загол. з екрану

20. ВІДДАЛЕНЕ ВИКОНАННЯ КОДУ [Електронний ресурс] / Wikipedia.- <https://cqr.company/ua/web-vulnerabilities/rce/> -23.03.2024 – Загол. з екрану

21. Rublon Autentification [Електронний ресурс] / Rublon.- <https://rublon.com/> - 1.01.2024 – Загол. з екрану

22. The NAT node [Електронний ресурс] / GNS3.- <https://docs.gns3.com/docs/using-gns3/advanced/the-nat-node/> - 1.01.2024 – Загол. з екрану

23. Set up or customize server backup [Електронний ресурс] / GNS3.- <https://learn.microsoft.com/en-us/windows-server-essentials/manage/set-up-or-customize-server-backup> - 05.19.2022 – Загол. з екрану

24. Protectimus Winlogon [Електронний ресурс] / Protectimus.- <https://www.protectimus.com/winlogon/index.php> - 01.01.2024 – Загол. з екрану

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				89
Змн.	Арк.	№ докум.	Підпис	Дата		

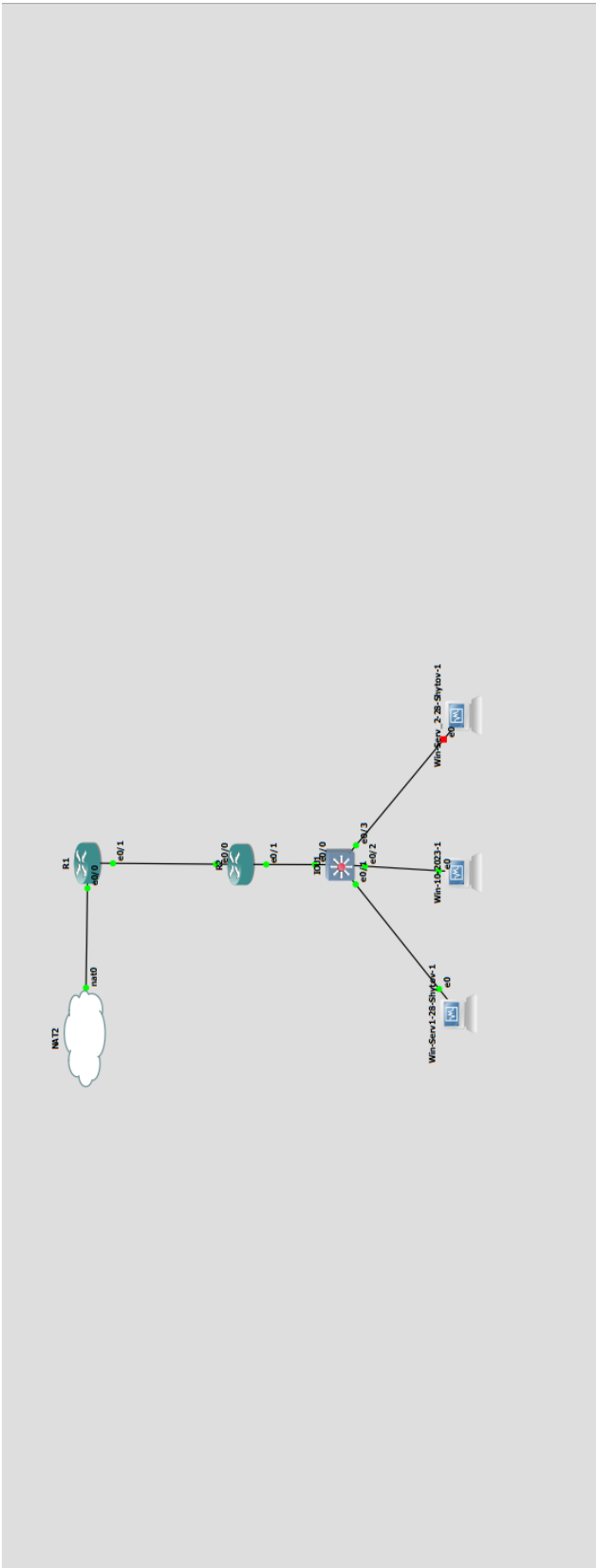
25. Securing Access, Authentication, and Identity Management On-Premises.
[Електроний ресурс] / RSA.- <https://www.rsa.com/products/securid/> -
01.01.2024 – Загол. з екрану
26. Тези Шитов Євгеній “CONSIDERATION OF THE PACKAGE OF NECESSARY TECHNOLOGIES FOR BUILDING THE ORGANIZATION’S LOCAL NETWORK”.
[Електроний ресурс] / Ztu.edu.ua.- <https://conf.ztu.edu.ua/wp-content/uploads/2024/05/126-1.pdf> - 25.04.2024 – Загол. з екрану
27. What's new in Windows Server 2019 [Електроний ресурс] / Microsoft.-
<https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2019>- 04.02.2024 – Загол. з екрану
28. What's new in Windows Server 2019 [Електроний ресурс] / Microsoft.-
<https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2019>- 04.02.2024 – Загол. з екрану
29. Domain Name System [Електроний ресурс] / Wikipedia.-
https://en.wikipedia.org/wiki/Domain_Name_System – Загол. з екрану

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		90

ДОДАТКИ

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				91
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема створеної мережі



		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				92
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинг конфігурації мережевих пристроїв

R1

conf t

int e0/0

ip nat outside

exit

int e0/1

ip nat inside

exit

ip nat inside source list 1 interface e0/0 overload

access-list 1 permit any

int e0/0

ip address dhcp

no sh

int e0/1

ip address 10.1.1.254 255.255.255.0

no sh

ex

router ospf 1

network 10.1.1.0 0.0.0.255 area 0

default-information originate

end

R2

conf t

int e0/0

ip address 10.1.1.1 255.255.255.0

no sh

exit

ip route 0.0.0.0 0.0.0.0 10.1.1.254

ip domain-lookup

ip name-server 8.8.8.8 8.8.4.4

router ospf 1

network 10.1.1.0 0.0.0.255 area 0

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		93

network 214.8.29.0 0.0.0.31 area 0

default-information originate

end

--lan network port configuration

conf t

int e0/1

ip address 214.8.29.1 255.255.255.224

no sh

end

wr

--dns

ip domain lookup

ip name-server 8.8.8.8 8.8.4.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		94

*E. Shytov, Student**I. Falkovskiy, Senior Lecturer, As. Prof.**Zhytomyr Polytechnic State University***“Consideration of the package of necessary technologies for building the organization's local network.”**

In today's rapidly evolving business landscape, the efficiency and reliability of local network infrastructure are paramount for streamlined operations. As organizations increasingly rely on digital connectivity, the importance of a robust network architecture cannot be overstated. To address the complexities inherent in network management, I embarked on a project to optimize our organization's local network by considering a comprehensive package of necessary technologies.

The project began with a meticulous evaluation to determine the optimal network architecture. After carefully considering various alternatives, we selected a framework built upon essential protocols and technologies, including VLAN, PVST+, HSRP, and IPv4 addressing, due to their compatibility and proven efficacy within our existing infrastructure.

A key focus of the project was refining network segmentation and resource allocation through VLAN protocols.

Implementing PVST+ was crucial in ensuring network redundancy and resilience. By managing separate spanning-tree instances for each VLAN, we mitigated the risk of network loops and expedited recovery during link failures, thereby minimizing disruptions and maintaining seamless connectivity.

HSRP was deployed to facilitate automatic failover between routers, further fortifying network availability. This mechanism ensured uninterrupted access to critical resources and services, enhancing the overall reliability of our network infrastructure.

In tandem with these protocols, meticulous attention was paid to IPv4 addressing strategies to streamline resource allocation and foster seamless communication across the network.

Additionally, paramount emphasis was placed on fortifying network security and integrity. Robust measures were implemented to safeguard against unauthorized access, potential data breaches, and network vulnerabilities.

In summary, this project represents a comprehensive approach to optimizing our organization's local network infrastructure. By considering a package of necessary technologies, including VLAN protocols, PVST+, HSRP, and IPv4 addressing, we aim to elevate network performance, bolster reliability, and enhance security measures, thereby facilitating seamless digital operations and sustained growth.

		Шитов Є.А			ККІКБ.КР.Б – 123 – 20 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		95