Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Методи шифрування даних в стані спокою в ОС Windows Server 2022"

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Швець Марта Андріївна
підпис (прізвище та ініціали)

Керівник Александер М. А.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Швець Марті Андріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Методи шифрування даних в стані спокою в ОС Windows Server 2022

Керівник роботи Александер Марек Богуслав Антонович, д.т.н., професор кафедри КБ.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 12.06.2024

3. Вихідні дані до роботи Вимоги до безпеки збережених даних. Операційна система Microsoft Windows Server 2022.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
1. Огляд предметної області
2. Можливості шифрування даних в стані спокою в операційній системі Windows
3. Налаштування та тестування методів шифрування в операційній системі Windows
4. Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Тема, мета, задачі.
Методи шифрування даних у стані спокою. Симетричні алгоритми шифрування. Потокове шифрування. Блокове шифрування. Можливості шифрування даних в стані спокою в операційній системі Windows. Налаштування доменних служб Active Directory та підвищення рівня сервера до контролера домену. Налаштування мережевих параметрів Windows 10 та Windows 11 та підключення до домену SBTNTU. Методи шифрування даних в операційній системі Windows. Використання BitLocker в Active Directory. Шифрування диску в Windows Server 2022. Шифрування диску в Windows 10 та Windows 11. Використання EFS в Active Directory. Шифрування файлів та каталогів в Windows.
Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С. Ю., к.т.н. доцент кафедри МТ		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01.2024	
2.	Опрацювання джерел в галузі дослідження	02.02 – 30.01	
3.	Оформлення розділу «Огляд предметної області»	21.02 – 10.03	
4.	Оформлення розділу «Можливості шифрування даних в стані спокою в операційній системі Windows»	11.03 – 25.03	
5.	Оформлення розділу «Налаштування та тестування методів шифрування в операційній системі Windows»	10.04 – 05.05	
6.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	10.05 – 21.05	
7.	Оформлення кваліфікаційної роботи	23.05 – 06.06	
8.	Нормоконтроль	06.06 – 10.06	
9.	Перевірка на плагіат	11.06 – 12.06	
10.	Попередній захист кваліфікаційної роботи	14.06 – 15.06	
11.	Захист кваліфікаційної роботи	25.06.2024	

Студент _____ Швець М. А.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Александер М. А.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Методи шифрування даних в стані спокою в ОС Windows Server 2022. // Кваліфікаційна робота ОР «Бакалавр» // Швець Марта Андріївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2024 // С. 76, рис. – 42, табл. – 0, кресл. – 13, додат. – 0.

Ключові слова: Windows, ADDS, BitLocker, EFS, ADCS, AES-CBC, XTS-AES, RSA, manage-bde.

У кваліфікаційній роботі бакалавра було проведено аналіз різних станів даних та розглянуто заходи захисту для кожного з них. Досліджено алгоритм симетричного шифрування AES та його практичне застосування в операційній системі Windows. Розроблено лабораторне середовище для практичного дослідження методів шифрування, включаючи налаштування Windows Server 2022 з роллю ADDS та встановлення робочих станцій з Windows 10 та Windows 11. Показано ефективність вбудованих методів шифрування, таких як BitLocker та EFS, зокрема їх можливості та переваги, а також практичні аспекти їх використання.

Дослідження також включало налаштування групових політик в домені для автоматичного зберігання ключів відновлення BitLocker та встановлення додаткових методів захисту, таких як паролі та PIN-коди. Підтверджено коректність зберігання ключів відновлення BitLocker в Active Directory та ефективність служби сертифікації Active Directory (ADCS) для керування сертифікатами шифрування для захисту ключів EFS.

Отримані результати свідчать про ефективність та надійність вбудованих методів шифрування даних в операційній системі Windows з централізованим управлінням за допомогою Active Directory Domain Services на базі Windows Server 2022.

ANNOTATION

Methods of data encryption at rest in Windows Server 2022 OS. // Thesis of educational level "Bachelor"// Marta Shvets // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБ-41 // Ternopil, 2024 // P. 76, fig. - 42, tab. - 0, chair. - 13, added. -0.

Keywords: Windows, ADDS, BitLocker, EFS, ADCS, AES-CBC, XTS-AES, RSA, manage-bde.

In the bachelor's thesis, an analysis of various data states was carried out and protection measures for each of them were considered. The AES symmetric encryption algorithm and its practical application in the Windows operating system have been studied. A lab environment was developed for hands-on investigation of encryption methods, including setting up Windows Server 2022 with the ADDS role and installing workstations with Windows 10 and Windows 11. The effectiveness of built-in encryption methods such as BitLocker and EFS was demonstrated, including their capabilities and benefits, as well as practical aspects of their use.

The research also included configuring group policies in the domain to automatically store BitLocker recovery keys and installing additional security methods such as passwords and PINs. Validated the correctness of storing BitLocker recovery keys in Active Directory and the effectiveness of Active Directory Certificate Services for managing encryption certificates to protect EFS keys.

The obtained results demonstrate the effectiveness and reliability of the built-in data encryption methods in the Windows operating system with centralized management using Active Directory Domain Services based on Windows Server 2022.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 8
ВСТУП 10
РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ 12
1.1 Класифікація даних за їхнім станом 12
1.2 Алгоритми шифрування даних в стані спокою 17
1.3 Висновки до розділу 21
РОЗДІЛ 2 МОЖЛИВОСТІ ШИФРУВАННЯ ДАНИХ В СТАНІ СПОКОЮ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS 22
2.1 Схема лабораторного середовища 22
2.2 Встановлення та налаштування об’єктів LAN мережі 23
2.2.1 Встановлення та налаштування Windows Server 2022 ADDC 23
2.2.2 Встановлення та налаштування Windows 10 та 11 27
2.3 Методи шифрування даних в операційній системі Windows 30
2.3.1 Шифрування даних з використанням BitLocker 30
2.3.2 Шифрування даних з використанням EFS 33
2.4 Висновки до розділу 34
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕТОДІВ ШИФРУВАННЯ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS 36
3.1 Використання BitLocker в Active Directory 36
3.1.1 Налаштування групової політики 36
3.1.2 Шифрування диску в Windows Server 2022 43
3.1.3 Шифрування диску в Windows 10 та Windows 11 47
3.2 Використання EFS в Active Directory 53
3.2.1 Налаштування служби сертифікації Active Directory 53
3.2.2 Шифрування файлі та каталогів в Windows 57
3.3 Висновки до розділу 63
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ 65
4.1 Загальні вимоги безпеки з охорони праці для користувачів ПК 65
4.2 Захист людини від впливу іонізуючого випромінювання 68
ВИСНОВКИ 72

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ADDS — Active Directory Domain Services

EFS — Encrypting File System

ADCS — Active Directory Certificate Services

TLS — Transport Layer Security

VPN — Virtual Private Network

IPsec — Internet Protocol Security

L2TP — Layer 2 Tunneling Protocol

PPTP — Point-to-Point Tunneling Protocol

TCP — Transmission Control Protocol

UDP — User Datagram Protocol

SSTP — Secure Socket Tunneling Protocol

IKEv2 — Internet Key Exchange version 2

SSO — Single Sign-On

MFA — Multi-Factor Authentication

AES — Advanced Encryption Standard

DES — Data Encryption Standard

ADDC — Active Directory Domain Controller

TPM — Trusted Platform Module

TCG — Trusted Computing Group

CBC — Cipher Block Chaining

XTS — XEX-based Tweaked CodeBook Mode with CipherText Stealing

FEK — File Encryption Key

DDF — Data Decryption Field

DRF — Data Recovery Field

CSP — Cryptographic Service Provider

RSA — Rivest-Shamir-Adleman

PKI — Public Key Infrastructure

CA	—	Certificate Authorities
CRL	—	Certificate Revocation Lists
KSP	—	Key Storage Provider

ВСТУП

У сучасному світі дані стали важливим ресурсом, що відіграє ключову роль у багатьох сферах життя, включаючи бізнес, науку, медицину, технології та інші. У зв'язку з постійною загрозою несанкціонованого доступу проблема захисту даних є надзвичайно актуальною. Для забезпечення високого рівня безпеки необхідно використовувати надійні методи шифрування, які гарантують захист даних як у стані руху, так і у стані спокою.

Метою цього дослідження є аналіз та практична реалізація вбудованих методів шифрування даних в операційній системі Windows з акцентом на централізоване управління за допомогою ADDS на базі Windows Server 2022.

Основними задачами дослідження є:

- огляд існуючих станів даних в яких вони можуть перебувати;
- аналіз вбудованих методів шифрування даних в операційній системі Windows;
- огляд і вивчення основних можливостей та характеристик вбудованих методів шифрування, таких як BitLocker та EFS, доступних в операційних системах Windows.
- практична реалізація методів шифрування;
- налаштування та управління ADCS;
- проведення тестування та перевірки правильності налаштування засобів шифрування;
- оцінка ефективність використання вбудованих методів шифрування в операційній системі Windows.

Об'єктом дослідження є вбудовані методи шифрування даних в операційній системі Windows, такі як BitLocker та EFS, а також служба сертифікації Active Directory (ADCS).

Предметом дослідження є практична реалізація методів шифрування даних в стані спокою з використанням зазначених технологій та інструментів.

Одержані результати дослідження можуть мати важливе практичне значення для організацій, що використовують операційні системи Windows у

корпоративному середовищі. Вони дозволяють забезпечити надійний захист конфіденційної інформації за допомогою вбудованих засобів шифрування, забезпечуючи централізоване управління та зберігання ключів шифрування BitLocker в Active Directory, а також видачу та керування сертифікатами з використанням служби ADCS при використанні EFS. Такий підхід дозволяє забезпечити високий рівень безпеки та зручності управління даними в організації.

РОЗДІЛ 1 ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Класифікація даних за їхнім станом

Дані - це інформація, яку можна записати, зберегти і обробити за допомогою комп'ютерних систем або інших технічних засобів. Вони можуть представляти собою числа, тексти, зображення, звуки або будь-яку іншу форму інформації, яка має сенс для конкретного контексту.

Дані можуть бути структурованими, наприклад, як таблиці у базі даних, або неструктурованими, такими як текстові документи, фотографії, відео тощо.

Ця інформація може бути оброблена, проаналізована і використана для різноманітних цілей, включаючи прийняття рішень, проведення досліджень, автоматизацію процесів, розробку продуктів і послуг, аналіз трендів, забезпечення безпеки і багато іншого.

Дані в стані спокою (data at rest) - це дані, які зберігаються у системі або на пристрої, та у даному момент часу не використовуються для активних операцій або обробки. Вони можуть бути збережені на сервері, в базі даних, на жорсткому диску комп'ютера чи іншому пристрої збереження.

Дані в русі (data in transit/data in motion) - це дані, які знаходяться у процесі передачі або переміщення з одного місця до іншого. Це можуть бути дані, які передаються через мережу з одного комп'ютера на інший або дані, які обробляються на проміжному етапі в процесі передачі. Дані в дорозі зазвичай мають тимчасовий статус і не зберігаються довготривало в цьому стані. Ці дані можуть проходити через проміжний етап обробки або конвертації перед тим, як досягти свого кінцевого призначення.

Дані, що використовуються (data in use) - це дані, які завантажуються в пам'ять для виконання певних операцій, обробки, аналізу або інших дій. Це дані, які в даний момент часу активно залучені до якихось процесів або операцій, що відбуваються.

Дані постійно зазнають змін упродовж свого життєвого циклу і переходять через різні стани, поки не будуть повністю очищені. Наприклад, коли дані

зберігаються в базі даних, вони перебувають у стані спокою. При запиті клієнта дані передаються через мережу та перебувають у стані руху. Дані, що використовуються, є активними і можуть зберігатися в оперативній пам'яті комп'ютера, кеш-пам'яті ЦП або регістрах ЦП (див. рисунок 1.1).

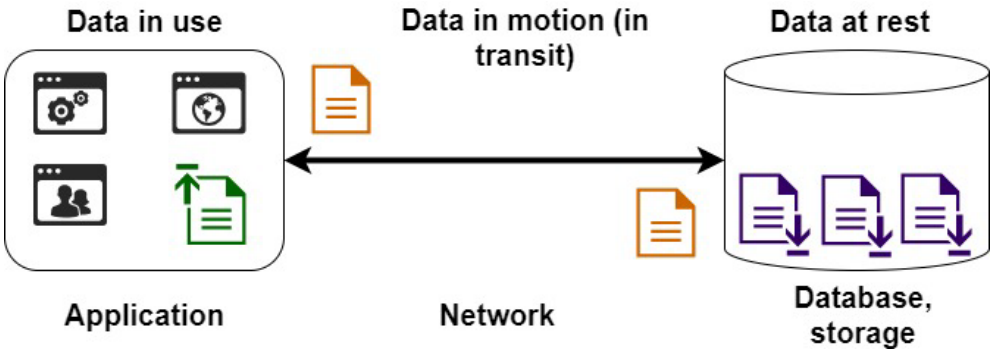

Рисунок 1.1 – Різні стани даних

Шифрування даних в русі - це процес застосування криптографічних методів для захисту конфіденційності та цілісності даних під час їх передачі через мережу [1]. Під час передачі даних через відкриті мережі, такі як Інтернет, існує ризик перехоплення чи зміни даних зловмисниками. Шифрування даних в русі допомагає запобігти таким загрозам, забезпечуючи безпеку під час передачі інформації. Під час шифрування даних в русі, оригінальні дані перетворюються у незрозумілий для сторонніх формат за допомогою різних методів шифрування. Цей процес забезпечує конфіденційність даних, оскільки зловмисники, які можуть перехопити дані у мережі, не зможуть прочитати їх без ключа розшифрування. Шифрування також допомагає у запобіганні модифікації даних під час передачі, оскільки будь-які зміни в зашифрованих даних стануть очевидними для отримувача, який може перевірити цілісність зашифрованих даних за допомогою контрольних сум або цифрових підписів.

Протокол TLS широко використовуються для захисту даних в русі в Інтернеті. TLS - це протокол, який забезпечує шифрування та автентифікацію даних під час їх передачі через мережу. Хоча TLS використовує криптографічні методи, щоб захистити дані, він сам по собі не є методом шифрування. Він використовує різні криптографічні алгоритми для забезпечення

конфіденційності, цілісності та автентифікації даних, а також забезпечення безпеки з'єднання між клієнтом і сервером.

TLS забезпечує шифрування даних під час їх передачі, а також використовує механізми для перевірки цілісності даних та автентифікації сторін, що спілкуються.

Використання VPN з шифруванням є одним з ефективних способів захисту даних в русі через мережу, зокрема через Інтернет. Коли використовується VPN з шифруванням з'єднання відбувається через зашифрований тунель між пристроєм і VPN-сервером. Це означає, що дані, відправлені через Інтернет, спочатку шифруються на пристрої, потім передаються через захищений канал до VPN-сервера, де вони розшифровуються і відправляються до їхнього кінцевого пункту призначення [2].

Шифрування даних у VPN тунелі ускладнює можливість перехоплення або читання інформації третіми сторонами [3].

Існує кілька протоколів VPN, які використовуються для забезпечення захищеного з'єднання між пристроями та мережами через Інтернет. Основні типи протоколів VPN включають [3]:

1) OpenVPN - це відкритий протокол VPN, який є одним з найпопулярніших і універсальних. Він підтримує як UDP, так і TCP для передачі даних, а також використовує різні криптографічні алгоритми для забезпечення конфіденційності та безпеки даних.

2) IPsec - це набір протоколів для захисту IP-трафіку шляхом шифрування та автентифікації даних. Він може використовуватися як для створення VPN-тунелей між мережами (site-to-site), так і для віддаленого доступу користувачів до мережі (client-to-site).

3) L2TP/IPsec - це комбінований протокол, який об'єднує функції L2TP для створення тунелів та IPsec для шифрування даних. Він часто використовується для віддаленого доступу користувачів до корпоративних мереж.

4) PPTP - це протокол, який шифрує дані, що передаються через VPN-тунель. Він використовує слабші методи шифрування порівняно з іншими протоколами, такі як Microsoft Point-to-Point Encryption.

5) SSTP - це протокол, розроблений компанією Microsoft, який використовує SSL/TLS для шифрування даних, переданих через VPN. Він часто використовується на платформах Windows.

6) IKEv2 - це протокол, який використовується для налаштування та управління безпечними асоціаціями ключів IPsec. Він підтримує автоматичне швидке перепідключення після втрати зв'язку.

7) WireGuard - це відносно новий протокол VPN, який був розроблений для створення безпечних з'єднань між пристроями через Інтернет. Він відрізняється від інших традиційних протоколів VPN, таких як OpenVPN або IPsec, тим, що пропонує простий та ефективний дизайн, а також високу швидкість та ефективність. WireGuard використовує сучасні криптографічні протоколи, такі як Curve25519 для обміну ключами і ChaCha20-Poly1305 для шифрування даних.

Перед початком фактичного використання даних вкрай важливо забезпечити їх безпеку. Для цього необхідно встановити надійний механізм автентифікації. Технології, такі як єдиний вхід (SSO) та багатофакторна автентифікація (MFA), можуть бути впроваджені для підвищення рівня безпеки. SSO спрощує процес автентифікації для користувачів та забезпечує безпеку та ефективність в управлінні доступом до різних ресурсів. MFA - це метод автентифікації, який вимагає від користувача надання додаткових, незалежних один від одного, елементів підтвердження своєї особи для доступу до системи. Зазвичай MFA включає комбінацію двох або більше елементів. Це може бути пароль, PIN-код або відповідь на контрольний питання. Додатково це може бути фізичний об'єкт, такий як ключ-картка або ключ USB, або генератор одноразових кодів. Також можливе використання біометричних елементів, таких як відбиток пальця, розпізнавання обличчя або розпізнавання голосу.

Використання кількох елементів підтвердження підвищує рівень безпеки, оскільки потенційний зловмисник повинен мати доступ до всіх елементів, щоб отримати доступ. Навіть якщо пароль користувача стає відомим, без доступу до інших елементів підтвердження, доступ до системи залишається неможливим. Якщо один з елементів автентифікації втрачений або скомпрометований, користувач може використовувати інші елементи автентифікації для

відновлення доступу. Деякі регуляторні стандарти та вимоги безпеки вимагають використання багатофакторної автентифікації для захисту конфіденційних даних.

Крім того, після проходження автентифікації користувача необхідно ретельно керувати доступом. Користувачам має бути наданий доступ лише до необхідних ресурсів для виконання їхніх завдань.

Дані, що використовуються, є вразливими до атак на автентифікацію. Ці види атак можуть використовуватися для отримання несанкціонованого доступу до даних шляхом обходу механізмів автентифікації, перехоплення облікових даних або інших методів [1].

Шифрування даних у стані спокою означає захист інформації, коли вона зберігається на носіях даних або в базі даних, і не використовується в даний момент [1]. Це важливий захисний механізм, оскільки даний стан може бути вразливим для атак, таких як несанкціонований доступ до даних.

Жодна всебічна стратегія захисту даних не є повною без шифрування в стані спокою. Компанія повинна захищати дані за допомогою шифрування, оскільки цей процес:

- блокує несанкціонований доступ до критично важливих даних, як зсередини, так і ззовні організації;
- не дозволяє зловмисникам легко ідентифікувати, інтерпретувати та викрасти цінні дані;
- обмежує поле дії в разі успішної атаки;
- захищає організацію при крадіжці чи втраті пристрою зберігання даних;
- запобігає спробам шантажу після викрадання даних.

Існують різні підходи до досягнення шифрування даних в стані спокою. Можливо розгорнути шифрування даних у стані спокою на чотирьох різних рівнях: шифрування на рівні програми, шифрування бази даних, шифрування файлової системи та повне шифрування диска.

Шифрування на рівні програми, яке змінює або генерує дані, застосовується на клієнтських робочих станціях або серверах. Цей вид шифрування ідеально

підходить для налаштування процесу шифрування для кожного користувача на основі їх ролей і дозволів.

Шифрування бази даних полягає в шифруванні всієї бази даних або певних її частин з метою збереження конфіденційності даних. Крім того, цей процес включає керування ключами шифрування та їх регулярну зміну для забезпечення додаткового рівня безпеки.

Шифрування файлової системи - це процес, який дозволяє адміністратору шифрувати лише обрані файлові системи або папки всередині файлової системи. Любий користувач може завантажити пристрій із цим шифруванням, але для доступу до захищених файлових систем потрібно ввести пароль або мати ключ чи сертифікат.

Повне шифрування диска перетворює всі дані на жорсткому диску в беззмістовну форму. Єдиний спосіб завантажити пристрій - ввести пароль для розшифрування даних. Цей метод шифрування є найнадійнішою формою захисту даних на пристрої.

Під час зберігання резервних копій даних потрібно використовувати шифрування, щоб захистити їх від несанкціонованого доступу. Алгоритми шифрування можуть бути однаковими для різних підходів.

1.2 Алгоритми шифрування даних в стані спокою

Алгоритми шифрування даних в стані спокою включають в себе різноманітні криптографічні методи, які використовуються для захисту інформації, коли вона знаходиться в стані спокою і не використовується [5].

В основному використовується симетричне шифрування для захисту даних в стані спокою (data at rest). У цьому випадку один ключ використовується як для шифрування, так і для розшифрування даних [6] (див рисунок 1.2).

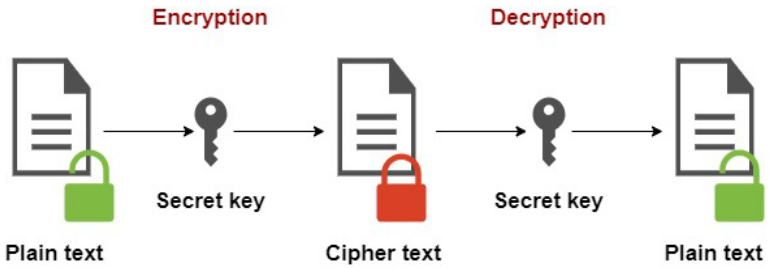

Рисунок 1.2 – Симетричне шифрування

Симетричні алгоритми шифрування зазвичай працюють дуже швидко, оскільки вони вимагають меншої кількості обчислень порівняно з асиметричними алгоритмами. Вони ефективні для шифрування великих об'ємів даних, оскільки використовується той самий ключ для кожного блоку даних. За допомогою симетричного шифрування можна забезпечити конфіденційність даних, оскільки доступ до розшифрованих даних можливий лише за наявності вірного ключа. Однак однією з основних проблем симетричного шифрування є проблема безпечного обміну секретним ключем між відправником і одержувачем. Це може бути особливо складно здійснити в відкритих мережах.

Симетричне шифрування може бути реалізоване у двох основних режимах: блоковому і потоковому [6]. Обидва режими використовують один і той же ключ для шифрування та розшифрування даних, але вони відрізняються у способі обробки даних.

У потоковому шифруванні дані шифруються окремими байтами або бітами з використанням ключа. Кожен біт або байт даних зазвичай обробляється окремо алгоритмом шифрування і вихідний шифротекст генерується в процесі обробки даних. Потокове шифрування може бути швидшим і більш ефективним для шифрування потоків даних, таких як мережевий трафік або потокове відео. Прикладом потокових шифрів є RC4, Salsa20, Grain, A5/1, ISAAC, HC-128, Grain-128, Fortuna та ChaCha20.

У блоковому шифруванні повідомлення розбивається на блоки фіксованого розміру, які шифруються окремо. Кожен блок даних вводиться в алгоритм шифрування разом з ключем, і вихідний шифротекст генерується на основі цього блоку. Заголовки додатково можуть містити вектор ініціалізації (IV), який використовується для забезпечення унікальності шифротексту.

Популярні блокові шифри включають AES, DES, Triple DES (3DES), Blowfish, Serpent, Twofish, Camellia [7].

AES шифрує та розшифровує дані блоками фіксованої довжини 128 біт. Розмір ключа може бути 128, 192 або 256 біт. Кількість раундів залежить від розміру ключа: для 128-бітного ключа - 10 раундів, для 192-бітного - 12 раундів, для 256-бітного - 14 раундів. Кожен раунд включає послідовність операцій: підстановку (Substitution), перестановку (Permutation), зсув (Shift) та лінійне перетворення (MixColumns) для обробки даних.

DES - це симетричний блоковий шифр, розроблений у 1970-х роках. Він був прийнятий Національним інститутом стандартів і технологій (NIST) як федеральний стандарт шифрування для захисту інформаційних систем у США. DES працює з блоками даних фіксованого розміру (64 біти) та використовує ключ довжиною 56 біт для шифрування і розшифрування даних. Незважаючи на свою популярність та широке використання у минулому, DES вважається застарілим з точки зору безпеки, оскільки його короткий ключ може бути легко зламаний за допомогою сучасних методів криптоаналізу. Тому зараз він зазвичай не використовується в критичних системах, і його використання рекомендується замінити на більш безпечні алгоритми, такі як AES.

Triple DES - це розширення стандарту DES, яке було введене для підвищення безпеки шифрування даних. Основна ідея полягає в тому, щоб застосовувати DES тричі з різними ключами для кожного застосування.

Дані спочатку шифруються за допомогою одного ключа DES, потім розшифровуються за допомогою другого ключа DES і, нарешті, ще раз шифруються за допомогою третього ключа DES. Розшифрування відбувається в зворотному порядку.

3DES має довжину ключа 168 біт (56 біт на кожен ключ), але фактична міцність шифрування вважається еквівалентною ключу довжиною 112 біт, оскільки перший ключ може бути такий самий, як і третій. Це зроблено для забезпечення сумісності зі стандартом DES. 3DES був популярним і широко використовуваним протягом багатьох років як альтернатива DES. Однак, через

обмежену швидкодію та зростаючі вимоги до безпеки, він витіснився більш сучасними алгоритмами шифрування, такими як AES.

Blowfish - це симетричний блоковий шифр, що шифрує та розшифровує дані блоками фіксованої довжини 64 біти. Blowfish дозволяє використовувати ключі різного розміру, від 32 до 448 біт. За замовчуванням використовується 16 раундів шифрування, в кожному з яких застосовуються операції заміни, перестановки та операції XOR для обробки даних. Хоча Blowfish досі застосовується в деяких системах, він поступово замінюється AES, який вважаються більш безпечними та ефективними.

Serpent є симетричним блочним шифром, який був розроблений як кандидат на роль стандарту AES. Він шифрує та розшифровує дані блоками фіксованої довжини 128 біт та підтримує ключі розміром 128, 192 та 256 біт. Застосовується 32 раунди шифрування, кожен з яких включає послідовність операцій підстановки, перестановки та операцій XOR для обробки даних. Незважаючи на те, що Serpent не став стандартом AES, він використовується в деяких системах як альтернатива AES.

Twofish - це симетричний блоковий шифр. Він був одним із фіналістів конкурсу AES, але не був обраний стандартом. Тем не менше, Twofish вважається дуже надійним шифром і використовується в різних системах для забезпечення безпеки даних. Шифрує та розшифровує дані блоками фіксованої довжини 128 біт. Підтримує ключі різного розміру, але найпоширеніші розміри ключів - 128, 192 та 256 біт. Використовує 16 раундів шифрування, кожен з яких включає послідовність операцій, таких як заміни, перестановки та операції XOR для обробки даних.

Camellia - це симетричний блочний шифр, спільно розроблений японським інститутом стандартів і технологій та компанією Mitsubishi Electric. Він був прийнятий як стандарт шифрування у Японії та широко використовується як альтернатива AES. Camellia шифрує та розшифровує дані блоками фіксованої довжини 128 біт. Підтримує ключі розміром 128, 192 та 256 біт. Використовує 18 раундів шифрування для ключів розміром 128 біт, і 24 раунди для ключів розміром 192 або 256 біт. Є стійким до різних видів криптографічних атак і

вважається дуже надійним шифром. Camellia широко використовується у японських системах та за її межами, а також у різних областях, включаючи мережеве шифрування, сховища даних та інші застосування.

1.3 Висновки до розділу

В першому розділі було проведено огляд існуючих станів даних в яких вони можуть перебувати. Проведено детальний огляд даних в стані спокою, даних в стані руху та даних, що використовуються. Показано механізми захисту даних при різних станах, такі як використання протоколу TLS та шифрованого VPN для захисту даних в русі, використання MFA та SSO для захисту даних, що використовуються та використання шифрування даних в стані спокою.

Проведено огляд алгоритмів шифрування даних в стані спокою. Показано, що симетричне шифрування в блоковому режимі є основним методом шифрування даних в стані спокою. Проведено аналіз та наведено характеристики основних семеричних блокових шифрів таких як: AES, DES, 3DES, Blowfish, Serpent, Twofish, Camellia. Показано, що шифрування даних у стані спокою є важливим заходом для захисту конфіденційної інформації під час зберігання і неактивного використання. Це допомагає запобігти ризику втрати даних або несанкціонованого доступу до них.

РОЗДІЛ 2 МОЖЛИВОСТІ ШИФРУВАННЯ ДАНИХ В СТАНІ СПОКОЮ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

2.1 Схема лабораторного середовища

На рисунку 2.1 зображено лабораторну схему мережі, яка буде використана для налаштування ADDS з контролером домену Windows Server 2022 та робочими станціями з Windows 10 та Windows 11.

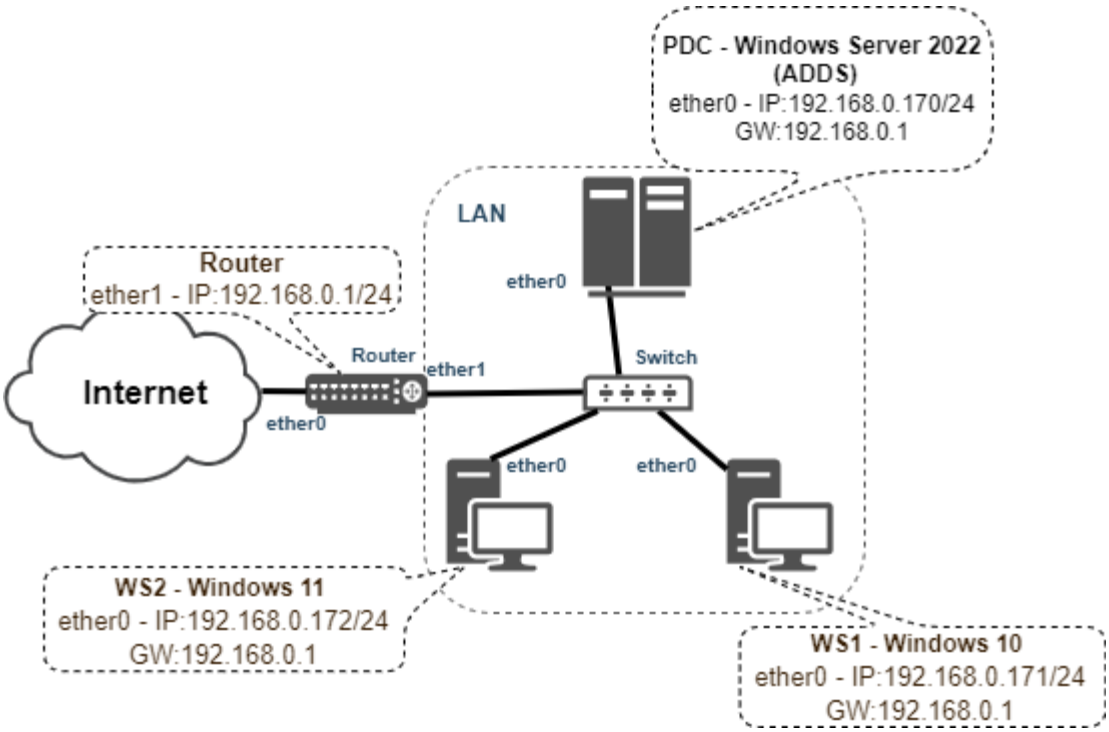

Рисунок 2.1 – Схема лабораторного середовища

На схемі показано, як різні пристрої взаємодіють один з одним. Маршрутизатор зображений як шлюз до інтернету, який має два з'єднання. Інтерфейс ether0 прямо підключений до інтернету, а ether1 з'єднується з внутрішньою мережею LAN.

Комутатор забезпечує з'єднання між кількома пристроями в мережі. До цього комутатора підключені два комп'ютери та сервер. Робоча станція WS1 з операційною системою Windows 10 з IP-адресою 192.168.0.171/24 та шлюзом за замовчуванням 192.168.0.1. Робоча станція WS2 з операційною системою Windows 11 з IP-адресою 192.168.0.172/24 та шлюзом за замовчуванням

192.168.0.1. Сервер PDC з операційною системою Windows Server 2022 є основним контролером домену Active Directory, з IP-адресою 192.168.0.170/24 та шлюзом за замовчуванням 192.168.0.1.

Кожен пристрій з'єднаний за допомогою Ethernet з'єднань і всі пристрої в мережі LAN використовують IP-адреси з однієї підмережі 192.168.0.0/24.

2.2 Встановлення та налаштування об’єктів LAN мережі

2.2.1 Встановлення та налаштування Windows Server 2022 ADDC

Windows Server 2022 ADDC є важливою складовою інфраструктури доменів Windows він відповідає за автентифікацію, авторизацію та керуванням об'єктами домену [8].

ADDS є роллю в операційній системі Windows Server 2022, яка надає служби директорії для організації та керування користувачами, комп'ютерами та іншими ресурсами в доменах. Основна функція ADDS - це забезпечення централізованого керування об'єктами в домені, а також надання механізмів автентифікації та авторизації користувачів і комп'ютерів.

Основні можливості ADDS включають:

1) Зберігання інформації про об'єкти (користувачі, комп'ютери, групи тощо) в дереві каталогів Active Directory.

2) Налаштування та застосування політик безпеки, доступу та аудиту для об'єктів домену.

3) Забезпечення реплікації даних між різними контролерами доменів для забезпечення високої доступності та надійності.

4) Надання послуг автентифікації та авторизації для користувачів і комп'ютерів у домені.

5) Підтримка інтеграції з іншими сервісами та додатками, такими як BitLocker та EFS.

ADDS є ключовою складовою інфраструктури Active Directory в операційних системах Windows Server 2022 і дозволяє організаціям керувати ресурсами та забезпечувати безпеку та доступність в мережі.

Після встановлення операційної системи Windows Server 2022 та налаштування статичних параметрів мережі (див. рисунок 2.2) наступним кроком є налаштування доменних служб Active Directory та підвищення рівня сервера до контролера домену.

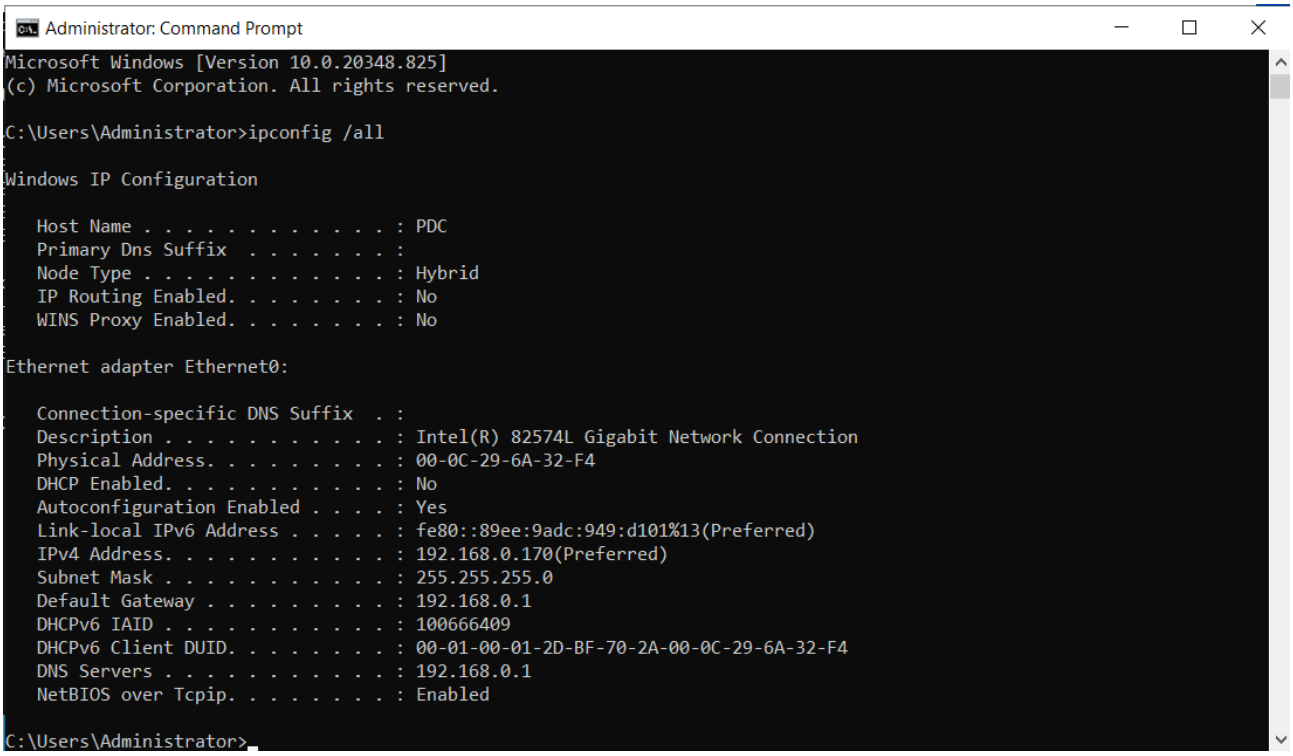

Рисунок 2.2 – Мережеві налаштування Windows Server 2022

На рисунку 2.3 показано процес встановлення ролі ADDS за допомогою команд в консолі PowerShell.

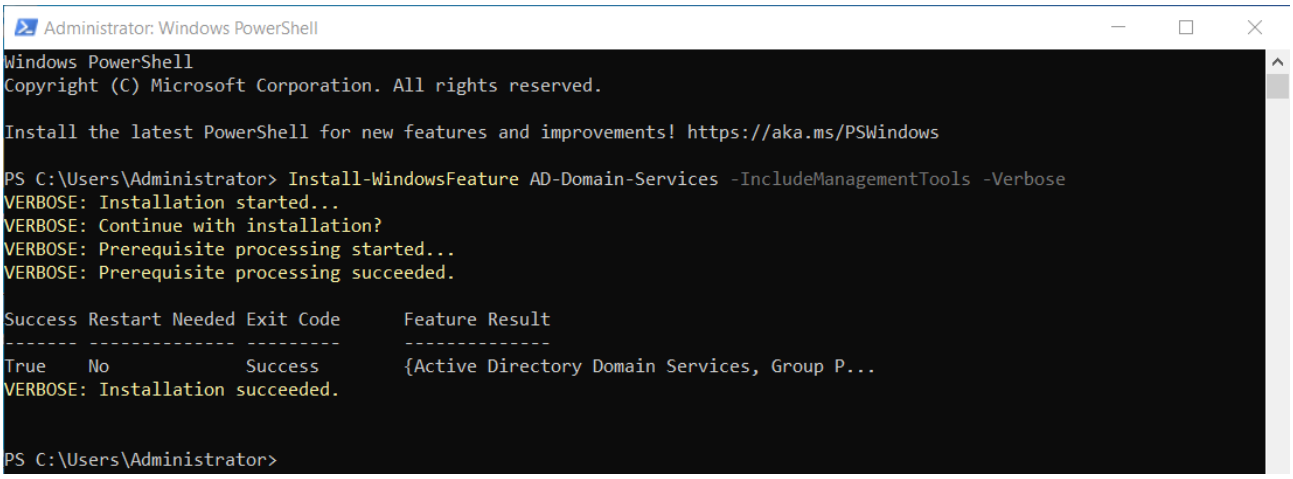

Рисунок 2.3 – Встановлення ролі ADDS в Windows Server 2022

Команда PowerShell встановлює роль ADDS на Windows Server 2022, включаючи також інструменти управління для цієї ролі. Опція `-Verbose` виводить додаткову інформацію про виконання команди.

На рисунку 2.4 показано вивід команди `PowerShell Get-WindowsFeature -Name *AD*`, яка призначена для отримання списку всіх встановлених або доступних для встановлення ролей та функцій Windows Server, які містять у своїх назвах AD. Це дозволяє швидко перевірити наявність будь-яких компонентів, пов'язаних з Active Directory.

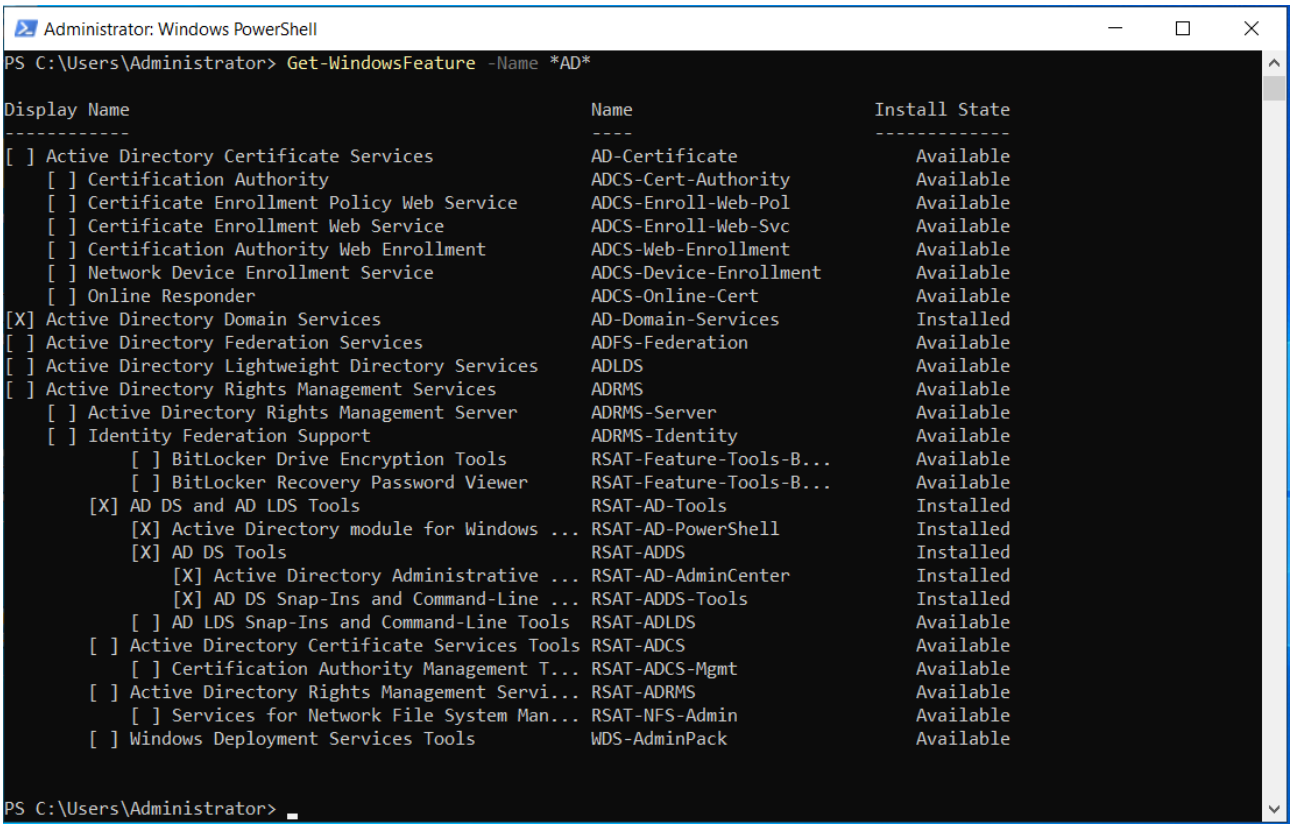

Рисунок 2.4 – Вивід команди PowerShell `Get-WindowsFeature -Name *AD*` в Windows Server 2022 ролі ADDS

Команда PowerShell `Install-ADDSForest -DomainName sbtntu.net -DomainNetbiosName SBTNTU -InstallDns:$true` встановлює новий ліс (forest) Active Directory з такими параметрами:

1) `-DomainName sbtntu.net` - вказує доменне ім'я, яке буде використане для нового лісу Active Directory, в даному випадку sbtntu.net.

2) `-DomainNetbiosName SBTNTU` - вказує NetBIOS-ім'я домену. У цьому випадку NetBIOS-ім'я встановлюється як SBTNTU.

3) `-InstallDns:$true` - вказує, що під час встановлення Active Directory також потрібно встановити службу DNS.

На рисунку 2.5 показано вивід команда PowerShell `Get-ADDomainController -Discover`, яка використовується для автоматичного виявлення всіх контролерів доменів у поточному домені.

Рисунок 2.5 – Вивід команди PowerShell `Get-ADDomainController -Discover` в Windows Server 2022

Команда виконує пошук і повертає інформацію про всі доступні контролери доменів, їхні IP-адреси, імена та інші важливі атрибути. Отримана інформація показує, що контролер домену з іменем PDC та IP-адресою 192.168.0.170 був виявлений в домені sbtntu.net.

2.2.2 Встановлення та налаштування Windows 10 та 11

Після встановлення операційних систем Windows 10 та Windows 11 потрібно здійснити статичні налаштування мережевих параметрів (див. рисунок 2.6-2.7).

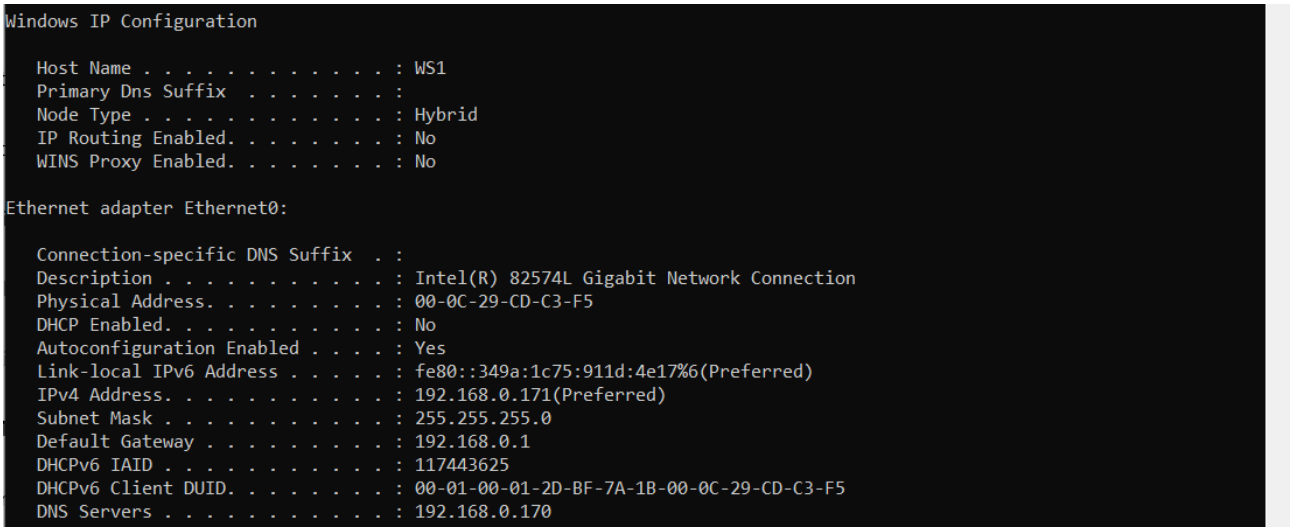

Рисунок 2.6 – Мережеві налаштування Windows 10

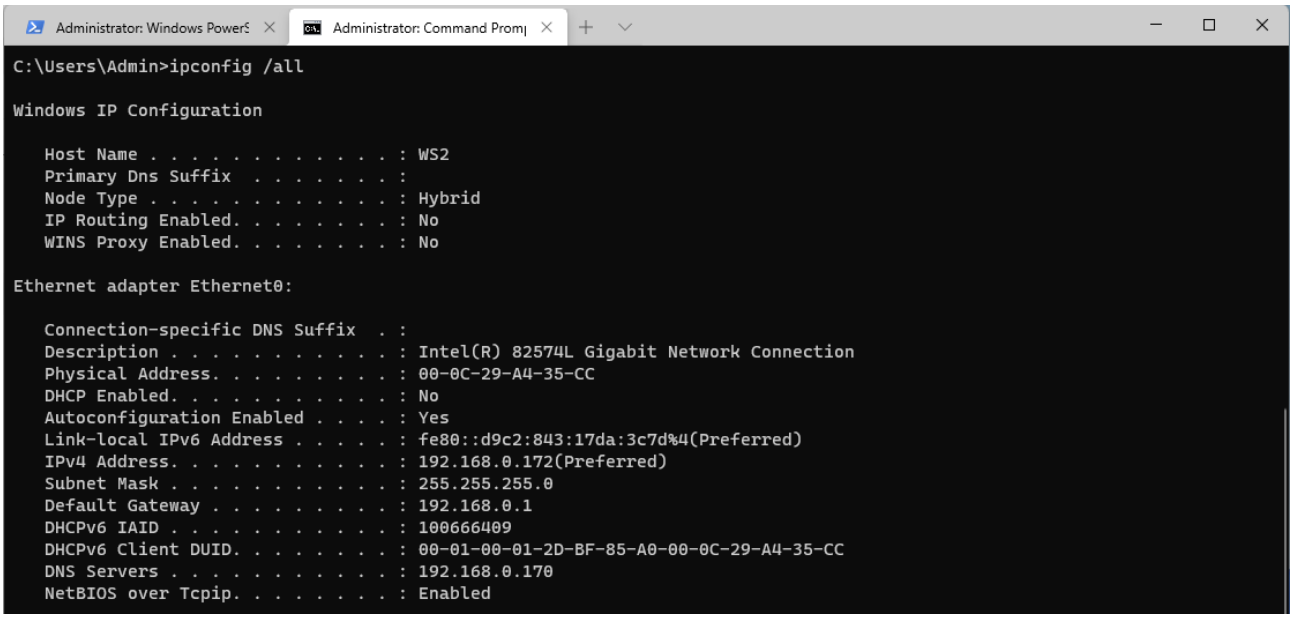

Рисунок 2.7 – Мережеві налаштування Windows 11

На рисунку 2.8 показано вивід команди, яка додає комп'ютер до домену з назвою SBTNTU за допомогою облікових даних адміністратора.

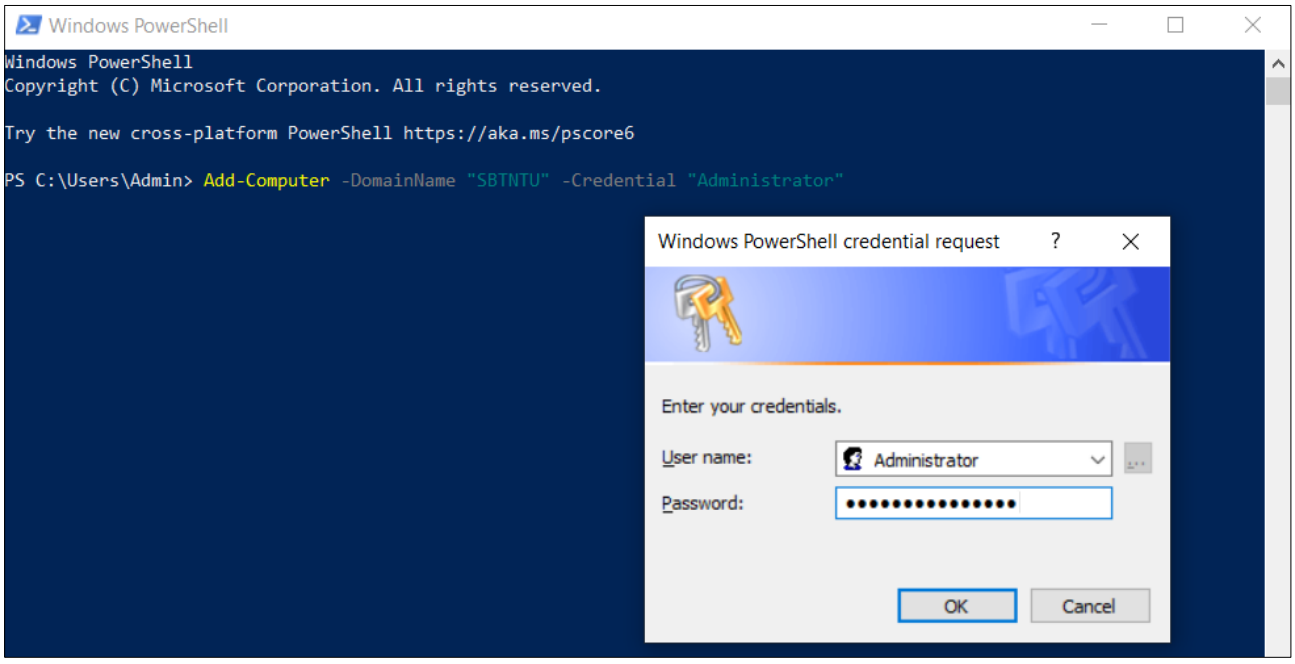

Рисунок 2.8 – Підключення Windows 10 до домену SBTNTU

Аналогічно додаємо комп’ютер з Windows 11 до домену SBTNTU.

На рисунку 2.9 показано вивід команди `Get-ADComputer -Filter *` на Windows Server 2022.

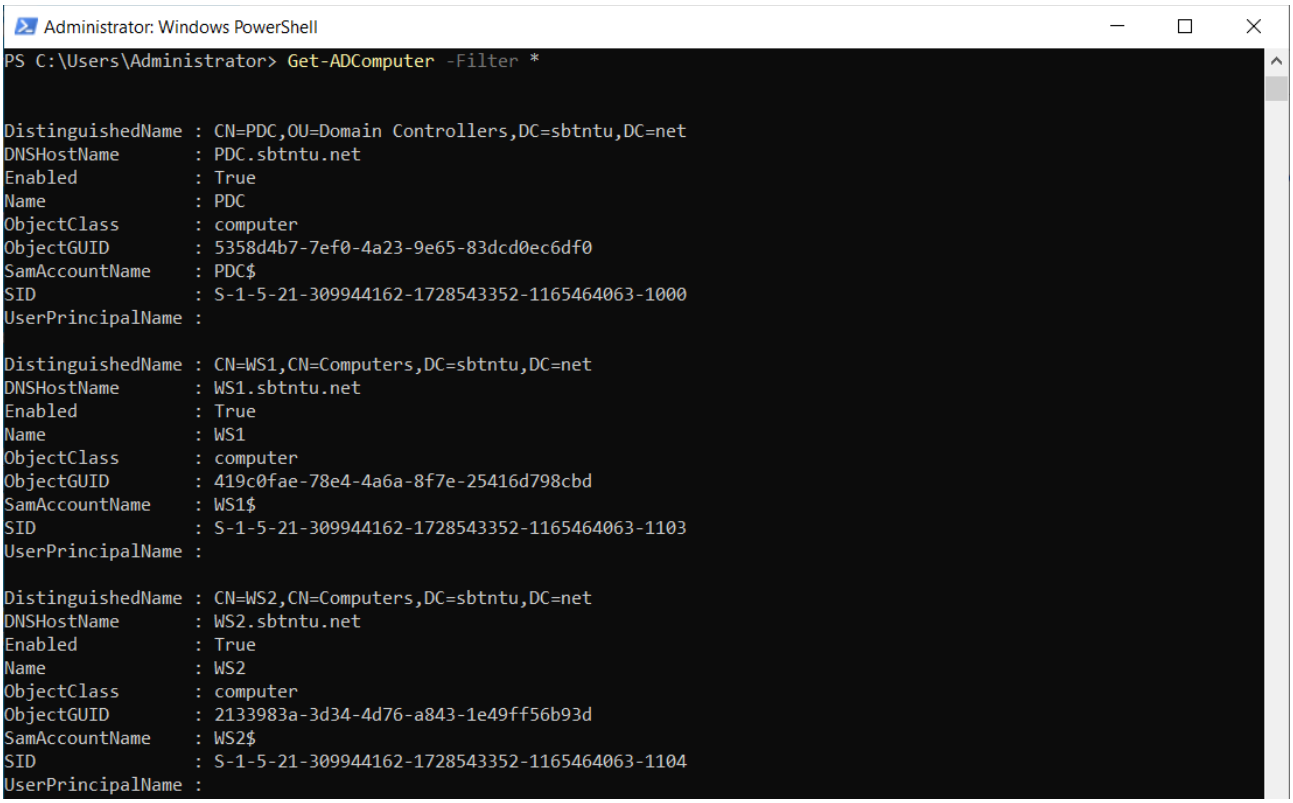

Рисунок 2.9 – Вивід команди `Get-ADComputer -Filter *` на Windows Server 2022

Ця команда виводить інформацію про комп'ютери в домені sbtntu.net.

Кожен запис містить таку інформацію:

1) `DistinguishedName` - це унікальне ім'я об'єкта, яке вказує на його розташування в структурі Active Directory. DN включає всі контейнери, в яких знаходиться комп'ютер, від самого кореня дерева AD до конкретного об'єкта.

2) `DNSHostName` - DNS-ім'я комп'ютера.

3) `Enabled` - показує, чи ввімкнений обліковий запис комп'ютера.

4) `ObjectClass` - клас об'єкта в Active Directory.

5) `ObjectGUID` - це унікальний ідентифікатор об'єкта, який допомагає однозначно ідентифікувати його в межах Active Directory.

6) `SID` - це унікальний ідентифікатор безпеки, який призначається кожному об'єкту в Active Directory і допомагає контролювати доступ до ресурсів.

Ця інформація дозволяє ідентифікувати та керувати комп'ютерами в домені. З виводу команди можна побачити, що комп’ютера з операційними системами Windows 10 та Windows 11 успішно додані до домену sbtntu.net.

2.3 Методи шифрування даних в операційній системі Windows

Шифрування даних в операційній системі Windows може бути здійснене за допомогою різних методів і технологій, що забезпечують захист конфіденційності інформації на різних рівнях [9].

BitLocker - це вбудований механізм шифрування диска в операційній системі Windows, який дозволяє шифрувати всі дані на жорсткому диску або вибрані томи [10]. BitLocker забезпечує захист від несанкціонованого доступу до даних у випадку втрати або крадіжки пристрою.

EFS - це інша вбудована функція операційної системи Windows, яка дозволяє шифрувати файли та каталоги на рівні файлової системи [11]. EFS дозволяє захистити конфіденційні дані, зберігаючи їх у зашифрованому вигляді на диску і розшифровуючи їх автоматично при доступі через авторизований обліковий запис.

2.3.1 Шифрування даних з використанням BitLocker

BitLocker - це функція безпеки в операційній системі Windows, яка забезпечує шифрування для цілих томів даних [10]. Це зменшує ризик розголошення конфіденційних даних через втрату, крадіжку або неналежне використання пристроїв. Дані на втраченому або викраденому пристрої можуть бути вразливими до несанкціонованого доступу. BitLocker робить дані недоступними, коли захищені пристрої виводяться з експлуатації або потрапляють у чужі руки.

BitLocker, у співпраці з модулем TPM, забезпечує максимальний рівень захисту для пристроїв Windows. Модуль TPM є стандартним апаратним компонентом, який вбудовується в пристрої Windows і працює з BitLocker, щоб

переконатися, що система не була змінена, коли вона перебуває у автономному режимі.

Окрім використання TPM, BitLocker може заблокувати звичайний процес завантаження, поки користувач не введе PIN або не підключить знімний пристрій, що містить ключ завантаження. Ці заходи безпеки забезпечують багатофакторну автентифікацію та гарантують, що пристрій не зможе запуститися або вийти зі сплячого режиму, поки не буде введено правильний PIN-код або не буде підключений правильний ключ завантаження.

На пристроях без TPM все ще можна використовувати BitLocker для шифрування диска операційної системи. У цьому випадку користувачу потрібно використовувати ключ завантаження, який може бути файлом, збереженим на знімному диску, що використовується для завантаження пристрою, або введенням пароля. Проте варіант використання пароля не є найбезпечнішим, оскільки він вразливий до атак грубої сили, і немає можливості блокування пароля. Тому параметр пароля за замовчуванням вимкнено і не рекомендується. Обидва варіанти не забезпечують перевірку цілісності системи перед завантаженням, яку забезпечує BitLocker із TPM.

Щоб використовувати перевірку цілісності системи, яку забезпечує TPM, пристрій повинен мати TPM версії 1.2 або новіше. Якщо TPM на пристрої відсутній, то обов'язковим стає зберігання ключа завантаження на знімному диску під час активації BitLocker. Також пристрій із TPM має мати прошивку BIOS або UEFI, яка сумісна з TCG. Ця прошивка встановлює ланцюжок довіри для запуску перед завантаженням, і вона повинна містити підтримку визначеного статичного кореня вимірювання довіри. Для комп'ютерів без TPM необхідна підтримка класу USB-накопичувачів та можливість читання файлів на таких накопичувачах під час завантаження у середовищі BIOS або UEFI.

BitLocker використовує алгоритм шифрування AES з ключем довжиною 128 або 256 біт. На пристроях з Windows 10 або новіших версіях підтримуються режими шифрування CBC або XTS. Для шифрування дисків операційних систем, фіксованих дисків даних і знімних дисків даних можна використовувати такі режими шифрування: AES-CBC 128, AES-CBC 256, XTS-AES 128 та XTS-AES

256 [12]. Режим XTS-AES 128 є режимом шифрування, який використовується за замовчуванням в BitLocker для шифрування даних на дисках. Якщо є потреба використовувати знімний диск на пристроях, які не працюють під керуванням Windows 10 або новіших версій, потрібно використовувати режим шифрування AES-CBC.

AES-CBC 128 - це режим шифрування, який використовує алгоритм AES з ключем довжиною 128 біт і режим шифрування CBC. У режимі CBC, перед тим як блок даних буде зашифрований, він комбінується з попереднім зашифрованим блоком даних шляхом використання операції побітового додавання (XOR). Перший блок в режимі CBC потребує вектора ініціалізації (IV), який є унікальним значенням і використовується для ініціалізації процесу шифрування. Для кожного наступного блоку в режимі CBC попередній зашифрований блок даних об'єднується операцією XOR з поточним блоком відкритого тексту перед його шифруванням. Це дозволяє кожному блоку даних впливати на шифрування наступного блоку, забезпечуючи унікальність кожного зашифрованого блоку. AES-CBC 256 використовує алгоритм AES з CBC та ключ довжиною 256.

XTS-AES 128 - це режим шифрування, який використовує алгоритм шифрування AES з режимом XTS та ключ довжиною 128 біт. Основна особливість режиму XTS полягає в тому, що він використовує два незалежних ключа для кожного блоку даних, що забезпечує безпеку шифрування при виконанні операцій з різними блоками даних. Один ключ використовується для блокового шифрування AES, а інший називається tweak value. Tweak додатково модифікується поліноміальною функцією Galois (GF) та застосовується операція XOR як до відкритого, так і до зашифрованого тексту кожного блоку. Функція GF забезпечує дифузію та гарантує, що ідентичні блоки даних не створюють однаковий зашифрований текст.

Головною метою режиму XTS є створення унікального зашифрованого тексту з відомим незашифрованим текстом без використання векторів ініціалізації або ланцюжків. Фактично, кожен блок майже подвійно зашифрований за допомогою двох незалежних ключів. Розшифрування даних відбувається як зворотній процес. Оскільки кожен блок є незалежним, і немає

ланцюжка, помилки шифрування в одному блоку не поширюються на інші блоки під час розшифрування. XTS-AES 256 використовує алгоритм AES з XTS та ключ довжиною 256.

Зберігання ключів відновлення BitLocker за допомогою Active Directory є надійним методом для централізованого управління ключами шифрування та забезпечення можливості їх швидкого відновлення.

2.3.2 Шифрування даних з використанням EFS

Шифрування файлів і папок за допомогою EFS є одним з методів шифрування в операційній системі Windows [11]. Використовуючи EFS, можна зашифрувати окремі файли або каталоги, щоб забезпечити їх конфіденційність. При використанні EFS ключі шифрування генеруються автоматично і зберігаються в захищеному сховищі, доступ до якого має лише користувач, який створює зашифровані файли. Під час використання EFS дані автоматично шифруються під час збереження на диск і розшифровуються під час доступу до них. EFS використовує симетричне шифрування для шифрування файлів та асиметричне шифрування для захисту ключів шифрування.

EFS виконує кілька кроків для шифрування файлу. Спочатку він генерує ключ шифрування файлу FEK. Потім використовується симетричний алгоритм з використанням FEK для шифрування файлу. Вибраний алгоритм може залежати від версії операційної системи, але в нових версіях Windows використовується AES. Після цього EFS отримує публічний ключ з сертифіката EFS, який знаходиться в профілі користувача.

Якщо сертифікат відсутній, Windows створює базовий сертифікат EFS від центру сертифікації підприємства (CA) у домені. Після цього EFS шифрує FEK публічним ключем користувача EFS та зберігає його в полі розшифровки даних DDF у заголовку файлу.

Кожен зашифрований файл має у своєму заголовку два окремі поля - поле розшифровки даних DDF та поле відновлення даних DRF. У DRF міститься зашифрований ключ, створений за допомогою сертифіката відновлення від

кожного агента відновлення. Коли користувач відкриває зашифрований файл, приватний ключ користувача розшифровує FEK у DDF, а потім FEK розшифровує сам файл. Якщо необхідно, агент відновлення також може розшифрувати файл за допомогою зашифрованого FEK у DRF. Тож лише користувач, який зашифрував файл, і будь-які призначені агенти відновлення можуть отримати доступ до файлу.

Пари публічних і приватних ключів для користувачів EFS і облікових записів агентів відновлення генеруються базовим постачальником криптографічних послуг Microsoft CSP, також відомим як базовий постачальник RSA. Публічні ключі та сертифікати за замовчуванням зберігаються в сховищі сертифікатів комп'ютера. Відповідні приватні ключі, які використовуються для розшифрування FEK, зберігаються у зашифрованому вигляді в профілях відповідних користувачів або облікових записах агентів відновлення даних у папці RSA.

RSA - це асиметричний криптографічний алгоритм, який використовується для шифрування та підпису повідомлень. Він базується на математичних операціях з факторизації великих простих чисел. Цей алгоритм використовує два ключі: публічний і приватний. Довжина ключів RSA вимірюється в бітах і зазвичай варіюється від 1024 до 4096 біт. Чим довший ключ, тим вищий рівень безпеки, але й вищі обчислювальні витрати. Оптимальним для безпеки вважається розмір ключа 2048 біт.

RSA є одним з найпоширеніших алгоритмів криптографії і залишається надійним засобом захисту даних в інформаційній безпеці.

2.4 Висновки до розділу

У другому розділі була розроблена лабораторна схема середовища для дослідження методів шифрування даних в стані спокою з використанням операційної системи Windows Server 2022.

Встановлено та налаштовано Windows Server 2022 з роллю ADDS. Також встановлено та налаштовано робочі станції з Windows 10 та Windows 11. Здійснено приєднання Windows 10 та Windows 11 до домену.

Описано вбудовані методи шифрування даних в операційній системі Windows. Наведено можливості BitLocker, які дозволяють шифрувати всі дані на жорсткому диску або вибраних томах та EFS, яка дозволяє шифрувати файли та каталоги на рівні файлової системи. Показано переваги застосування BitLocker з модулем TPM, що забезпечує максимальний рівень захисту для пристроїв Windows. Описано режими шифрування даних за допомогою BitLocker з використанням симетричних шифрів AES-CBC 128, AES-CBC 256, XTS-AES 128 та XTS-AES 256. Описано принцип роботи EFS в Windows. Показано, що EFS використовує симетричне шифрування AES для шифрування файлів та асиметричне шифрування RSA для захисту ключів шифрування.

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕТОДІВ ШИФРУВАННЯ В ОПЕРАЦІЙНІЙ СИСТЕМІ WINDOWS

3.1 Використання BitLocker в Active Directory

Захист конфіденційної інформації та безпека даних є пріоритетом для організацій будь-якого розміру. Щоб забезпечити безпеку даних на пристроях, таких як сервера та настільні комп’ютери, важливо використовувати надійні засоби шифрування. BitLocker, програма для шифрування дисків у Windows, надає ефективне рішення. Ця програма дозволяє зберігати ключі відновлення BitLocker в Active Directory. Збереження ключів відновлення BitLocker в Active Directory дозволяє централізовано керувати і забезпечувати доступ до них для відновлення даних в разі втрати пароля.

3.1.1 Налаштування групової політики

Для забезпечення збереження ключів відновлення в Active Directory потрібно налаштувати групові політики в домені так, щоб при використанні BitLocker для шифрування диска автоматично зберігалися ключі відновлення в обліковому записі комп'ютера в Active Directory.

Створимо групову політику BitLocker-Computer-Policy та застосуємо її до домену sbtntu.net.

На рисунку 3.1 показано встановлення політики, яка дозволяє налаштувати алгоритм та довжину ключа шифрування, які використовує BitLocker Drive Encryption.

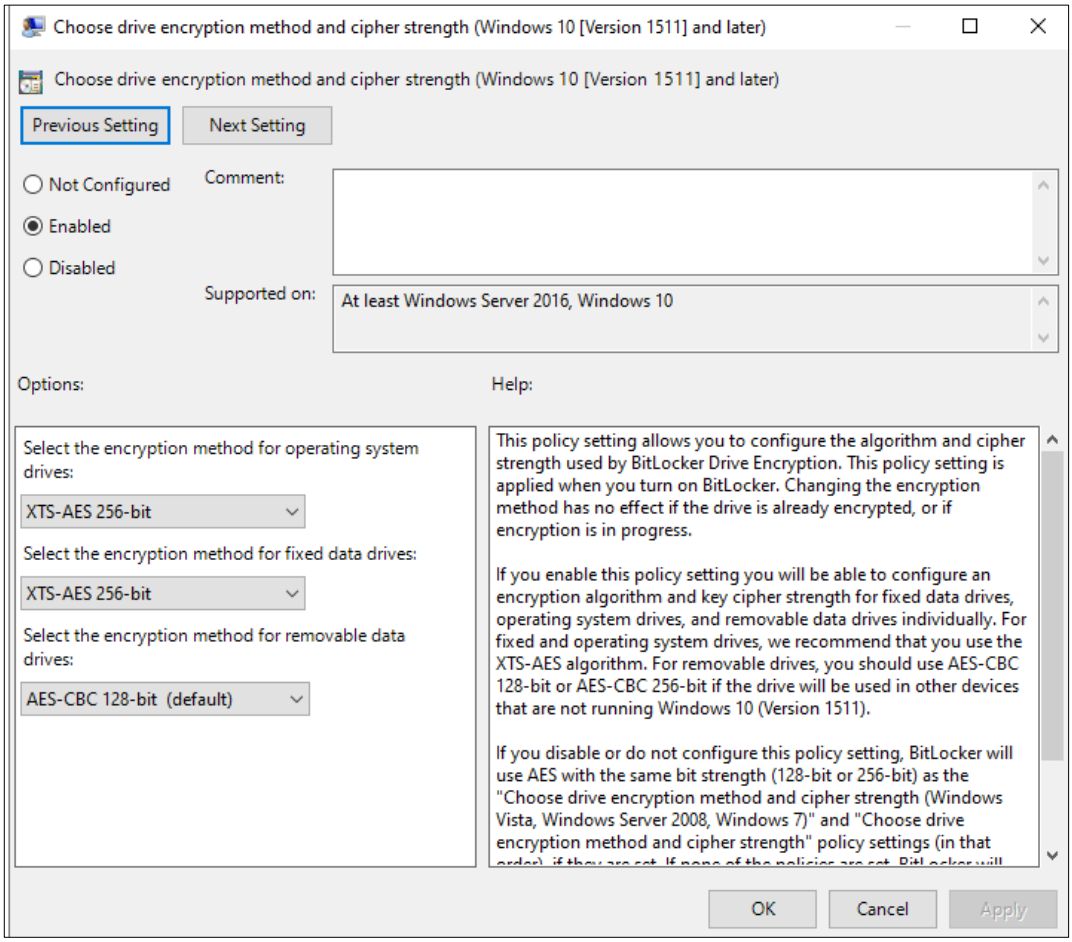

Рисунок 3.1 – Налаштування алгоритму та довжини ключа шифрування BitLocker

Це налаштування політики застосовується лише при увімкненні BitLocker. Якщо диск вже зашифрований або процес шифрування вже запущено, зміна методу шифрування не буде врахована. Є можливість налаштувати алгоритм шифрування та довжину ключа окремо для фіксованих дисків даних, дисків операційної системи і знімних дисків. Рекомендується використовувати алгоритм XTS-AES для фіксованих і системних дисків. Для знімних дисків потрібно використовувати AES-CBC, якщо диск буде використовуватися на пристроях, які не працюють під керуванням Windows 10 або новішої версії.

На рисунку 3.2 показано налаштування політики, яка дозволяє керувати резервним копіюванням інформації про ключі відновлення BitLocker в ADDS.

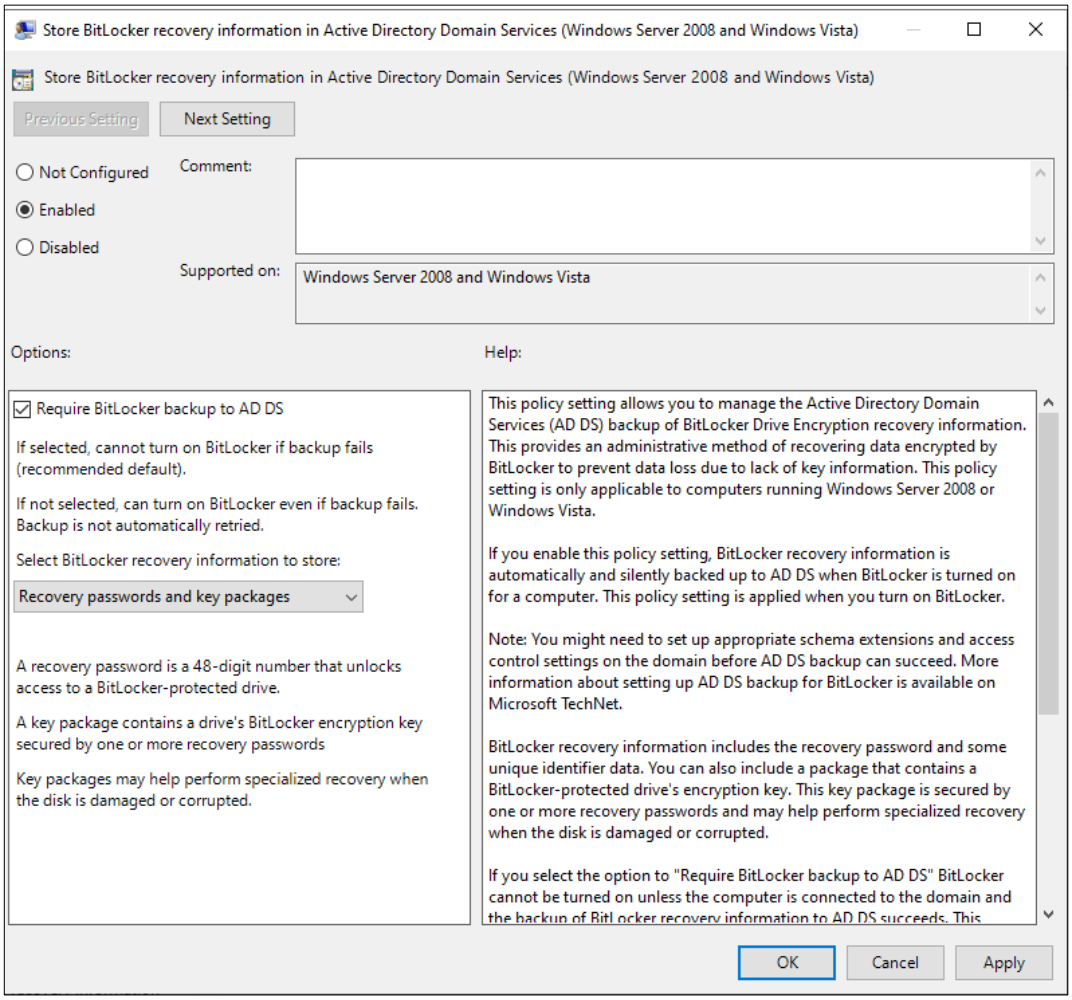

Рисунок 3.2 – Налаштування політики керування резервним копіюванням інформації для відновлення BitLocker

Ця настройка політики дозволяє забезпечити адміністративний метод відновлення даних, що були зашифровані за допомогою BitLocker, для запобігання можливим втратам інформації. Після активації цієї політики інформація про відновлення BitLocker автоматично зберігається в AD DS під час увімкнення BitLocker на комп'ютері. Ця настройка політики застосовується саме під час активації BitLocker. Інформація про відновлення BitLocker включає в себе пароль відновлення та різноманітні унікальні ідентифікатори.

Опція `Require BitLocker backup to ADDS` встановлює, що BitLocker не може бути увімкнено, якщо комп'ютер не має зв’язку з доменом або якщо резервне копіювання інформації про відновлення BitLocker в ADDS не вдалося. Ця опція включена за замовчуванням для забезпечення можливості відновлення BitLocker. Якщо опція вимкнена, спроба резервного копіювання в ADDS все

одно відбудеться, але проблеми з мережею або інші невдачі не зупинятимуть налаштування BitLocker. Резервне копіювання не повторюється автоматично і пароль відновлення не буде збережено в ADDS під час налаштування BitLocker.

На рисунку 3.3 показано налаштування політики, яка дозволяє керувати процесом відновлення зашифрованих за допомогою BitLocker фіксованих дисків даних. Опція `Allow data recovery agent` використовується для вказівки, чи може агент відновлення даних бути використаний з фіксованими дисками даних, зашифрованими за допомогою BitLocker.

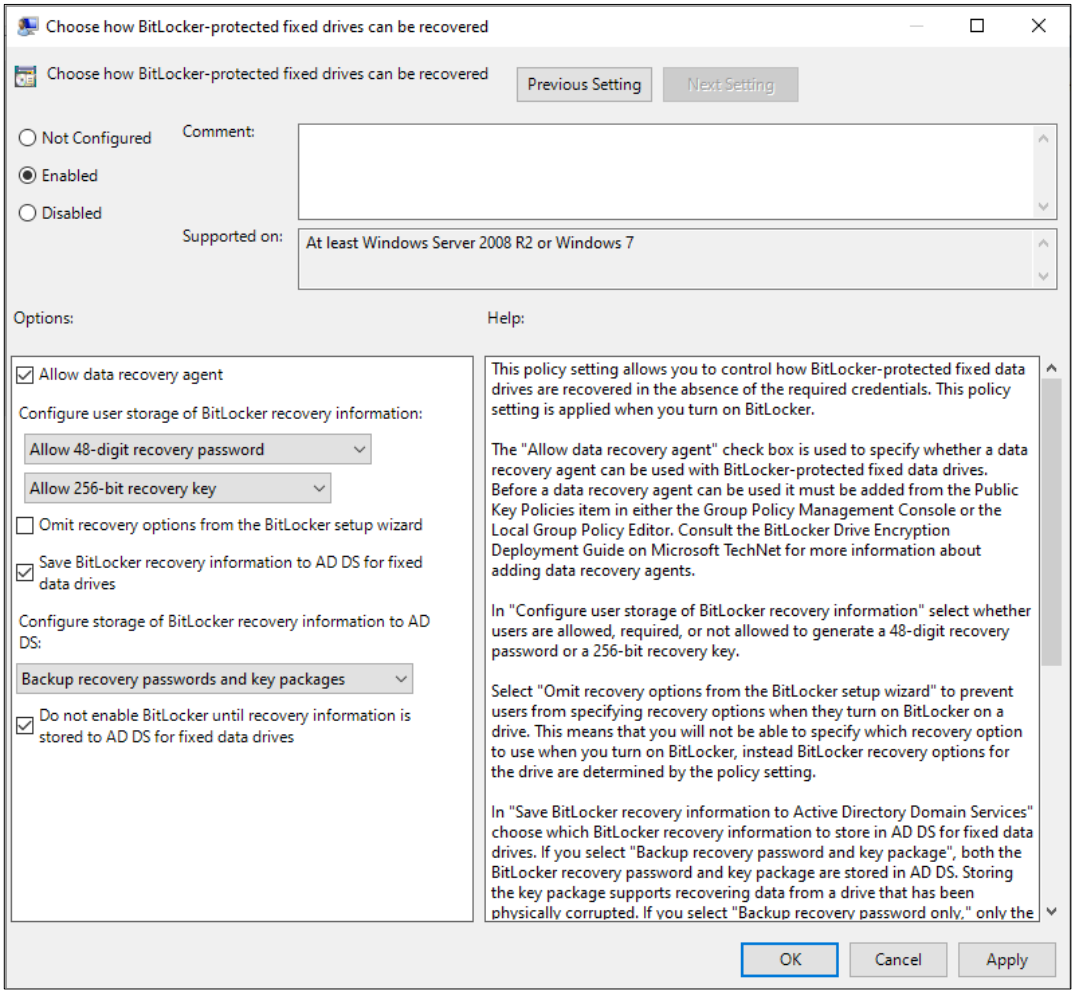

Рисунок 3.3 – Налаштування політики керувати процесом відновлення зашифрованих за допомогою BitLocker фіксованих дисків даних

Опція `Backup recovery password and key package`, встановлює зберігати в ADDS пароль відновлення і ключі BitLocker. Збереження пакета ключів допомагає відновленню даних з диску, який був фізично пошкоджений. Якщо

вибрати `Backup recovery password only`, в AD DS буде збережено лише пароль відновлення.

Опція `Do not enable BitLocker until recovery information is stored in AD DS for fixed data drives` забороняє користувачам увімкнення BitLocker, якщо комп'ютер немає зв’язку з доменом або резервне копіювання відомостей про відновлення BitLocker в ADDS не вдалося.

Аналогічні налаштування також проведено для дисків операційної системи і знімних дисків.

На рисунку 3.4 показано встановлення політики, яка дозволяє налаштувати, додаткову автентифікацію кожного разу при запуску комп'ютера з або без TPM.

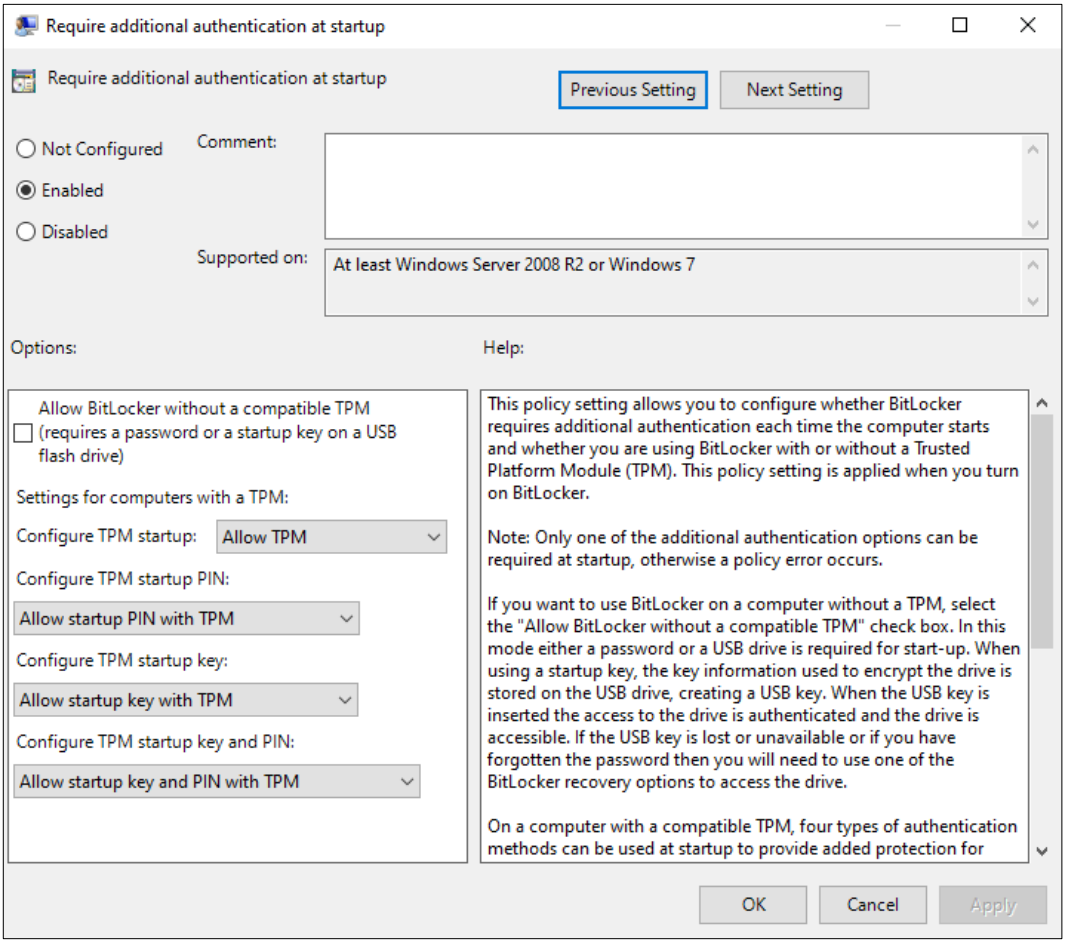

Рисунок 3.4 – Налаштування політики додаткової автентифікації для BitLocker диску операційної системи

На комп'ютері з TPM, для надання додаткового захисту зашифрованим даним під час запуску можна використовувати чотири типи методів

автентифікації. При запуску комп'ютера можна використовувати лише TPM для автентифікації, або також можна вимагати підключення USB-флеш з ключем запуску, введення 6-значного або 20-значного персонального ідентифікаційного номера (PIN) або обидва варіанти.

Якщо політика активована користувачі можуть налаштувати розширені параметри запуску у майстрі налаштування BitLocker.

На рисунку 3.5 показано консоль управління груповими політиками (GPMC) в Windows Server 2022, зокрема налаштування, які пов'язані з груповою політикою BitLocker-Computer-Policy.

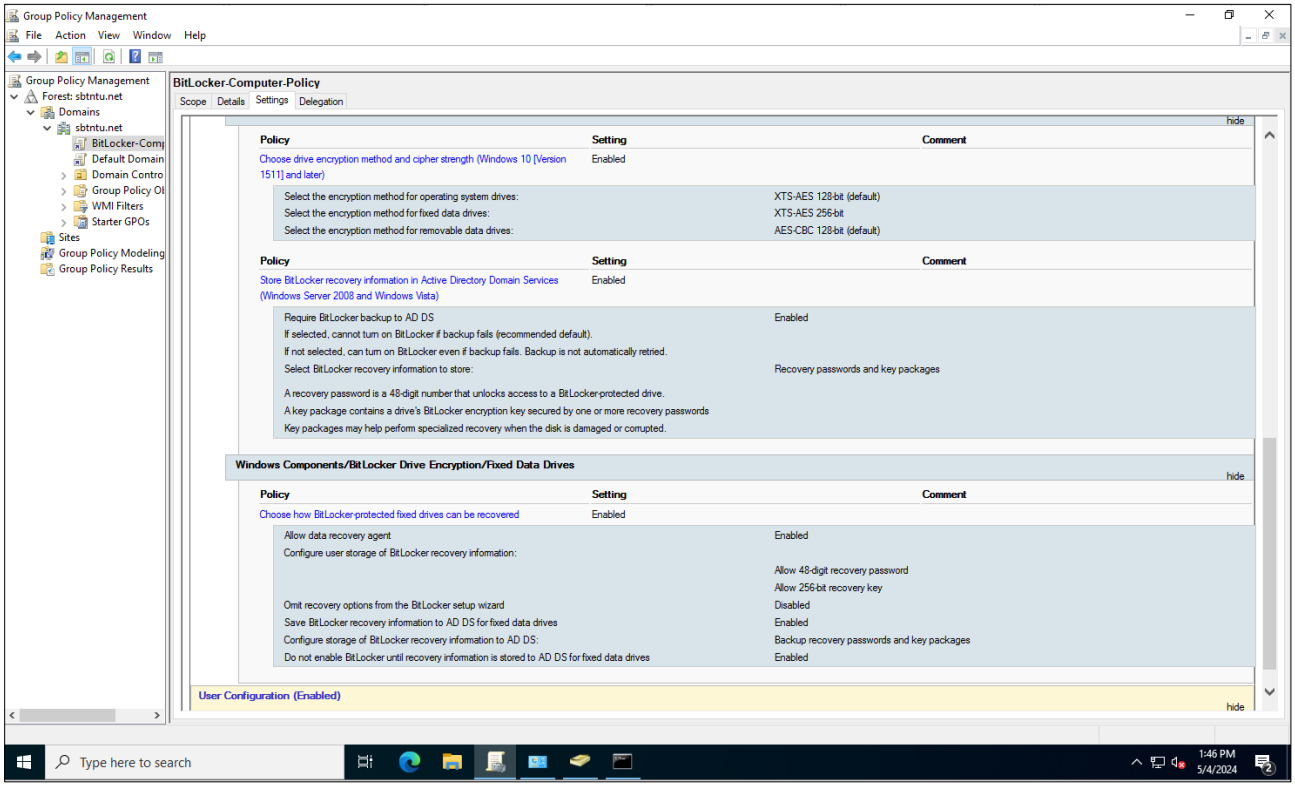

Рисунок 3.5 – Групова політика BitLocker-Computer-Policy в Windows Server 2022 ADDC

На рисунку 3.6 показано результати виконання команди оновлення та виводу результатів застосування групових політик в Windows Server 2022 ADDC.

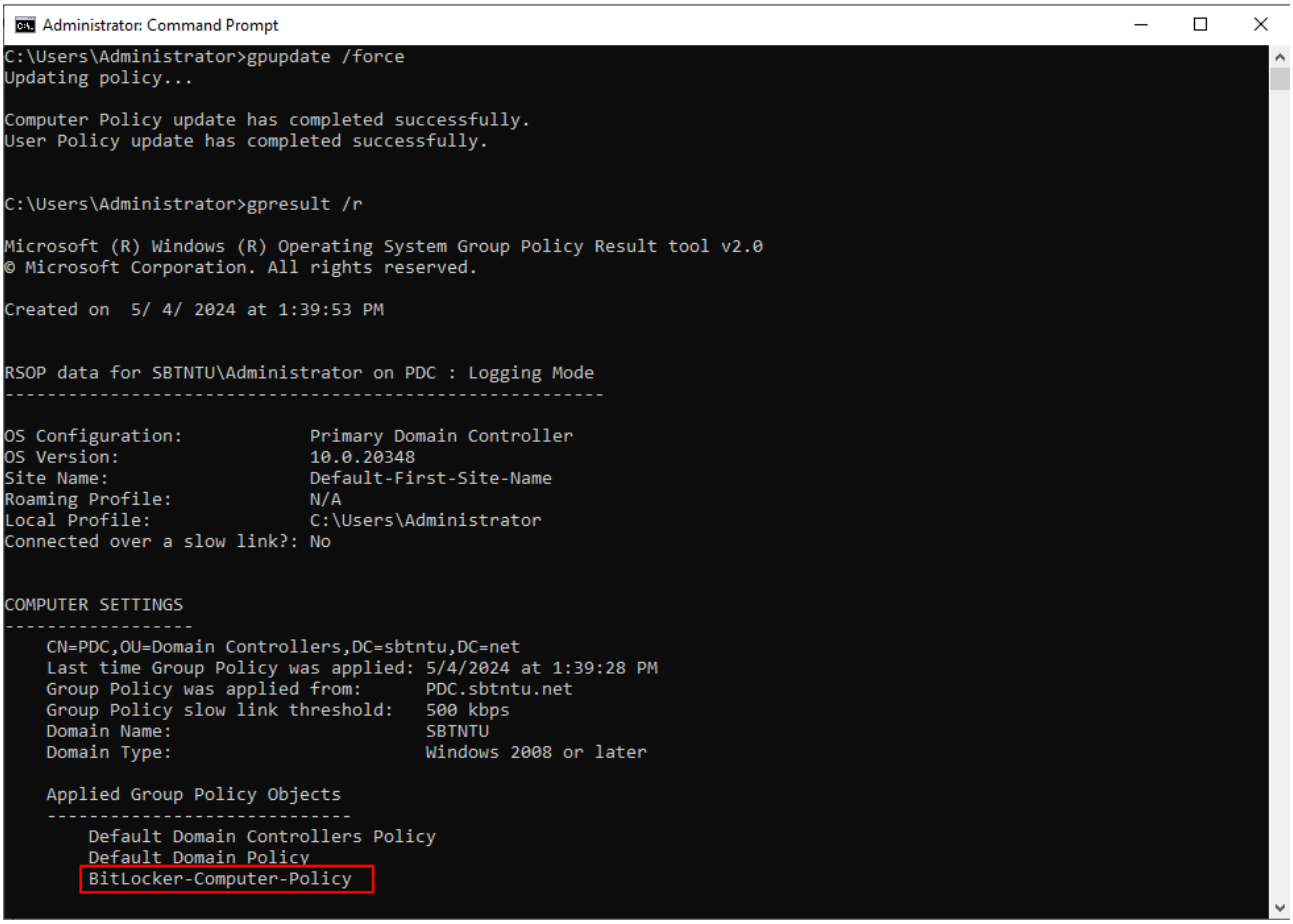

Рисунок 3.6 – Результати виконання команди `gpupdate /force` та `gpresult /r`

Команда `gpupdate /force` запускає примусове оновлення групових політик для комп'ютера та користувача. Вивід показує, що оновлення обох політик завершено успішно.

Команда `gpresult /r` відображає набір політик для поточного користувача та комп'ютера. Вона використовується для перевірки, які політики застосовані до системи та користувача. Групова політика BitLocker-Computer-Policy успішно застосована.

Для ефективного керування та налаштування BitLocker на клієнтських комп'ютерах необхідно встановити необхідні компоненти на Windows Server 2022 ADDC.

На рисунку 3.7 показано результати виконання команди PowerShell для встановлення BitLocker Drive Encryption на Windows Server 2022 ADDC та інструментів керування BitLocker.

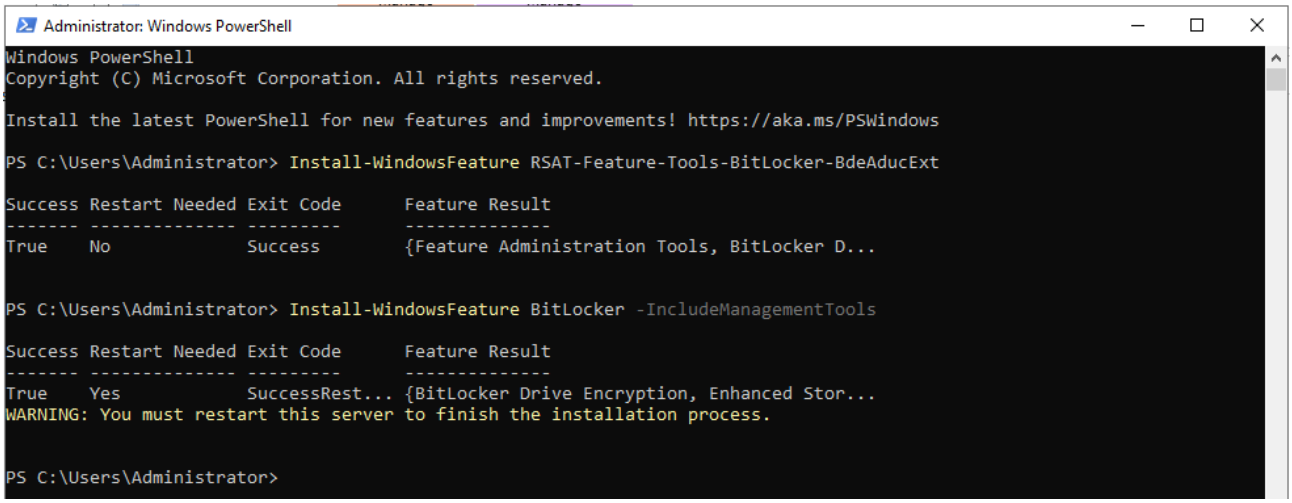

Рисунок 3.7 – Результати виконання команди встановлення BitLocker та інструментів керування BitLocker в Windows Server 2022 ADDC

Це дозволить адмініструвати ключі відновлення в Active Directory, що є важливою складовою забезпечення безпеки даних при відновленні BitLocker

3.1.2 Шифрування диску в Windows Server 2022

Виконаємо шифрування диску e: в операційній системі Windows Server 2022 за допомогою інструменту manage-bde [13]. Утиліта manage-bde - це інструмент управління шифруванням дисків BitLocker в операційних системах Windows. Він надає набір команд для налаштування, керування і моніторингу шифрування дисків, включаючи додавання та видалення захисних ключів, активацію та деактивацію шифрування, а також отримання інформації про статус шифрування дисків. За допомогою manage-bde можна виконувати різноманітні завдання, пов'язані з управлінням BitLocker, в тому числі додавання захисних ключів, встановлення паролів, налаштування політик безпеки, розблокування дисків і багато іншого.

На рисунку 3.8 показано вивід команди для перегляду статусу шифрування диска за допомогою утиліти manage-bde.

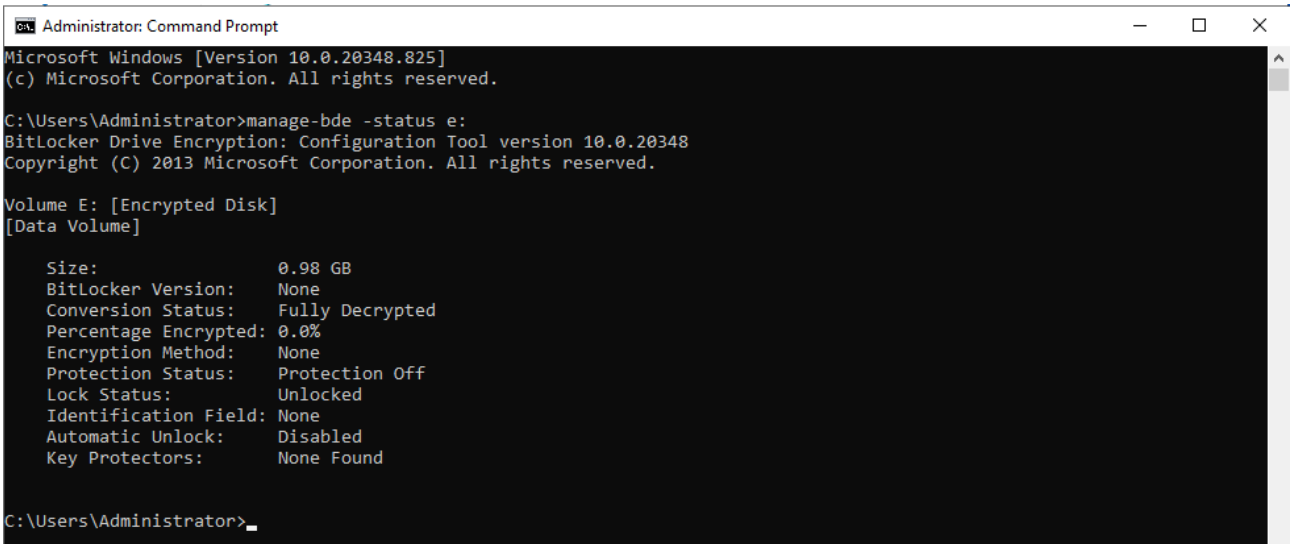

Рисунок 3.8 – Вивід команди `manage-bde -status e:` до запуску процесу шифрування BitLocker в Windows Server 2022

Ці дані вказують, що диск e: не зашифровано, шифрування для нього вимкнено, і жодних захистів ключів не налаштовано.

На рисунку 3.9 показано вивід команд увімкнення шифрування BitLocker та встановлення паролю розблокування диску за допомогою утиліти manage-bde.

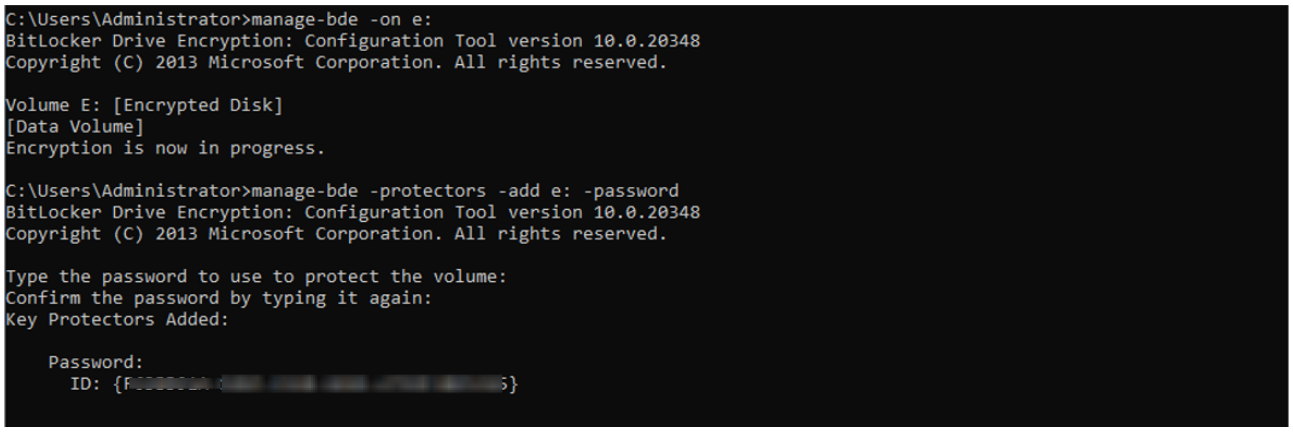

Рисунок 3.9 – Вивід команд увімкнення шифрування BitLocker та встановлення паролю розблокування диску в Windows Server 2022

Шифрування BitLocker для диска e: тепер активовано і захищено паролем.

На рисунку 3.10 показано вивід команд, яка використовується для додавання ключа відновлення (recovery password) до диску з літерою приводу e:.

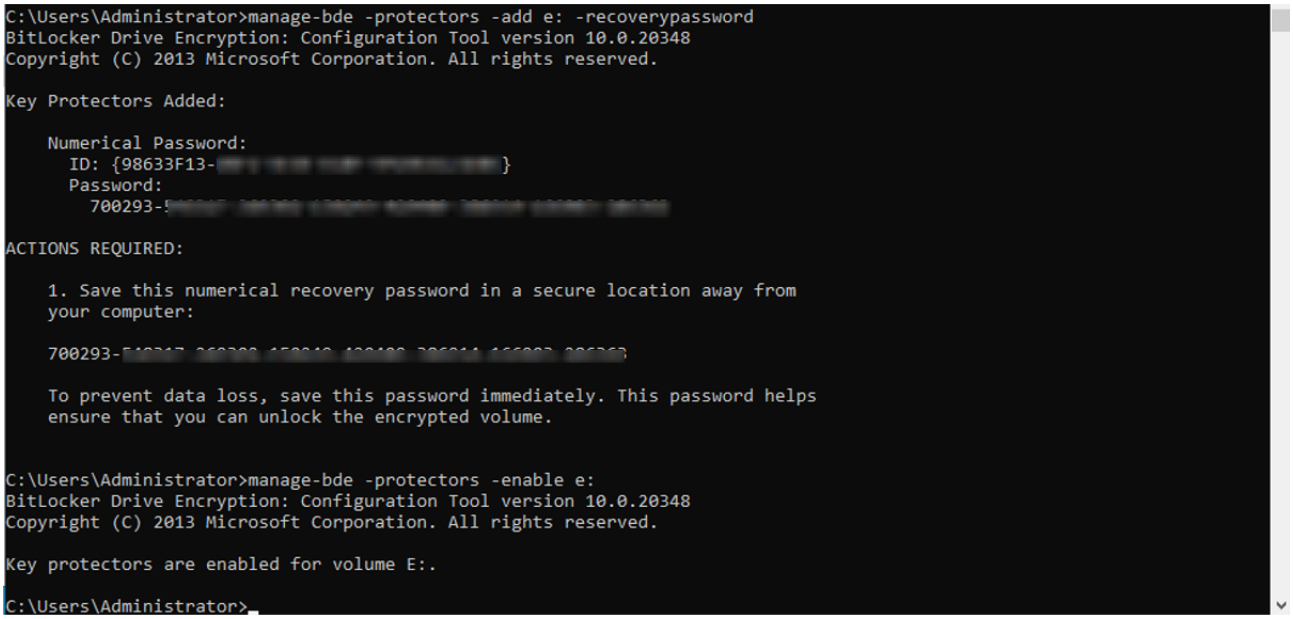

Рисунок 3.10 – Вивід команд додавання ключа відновлення BitLocker в Windows Server 2022

Ця команда дозволяє зберегти ключ відновлення, який можна використовувати для розблокування диску у випадку втрати основного пароля або інших проблем з доступом. Ключ відновлення є важливим інструментом для відновлення доступу до даних в разі непередбачених ситуацій.

На рисунку 3.11 показано вивід команди для перегляду статусу шифрування диска e: після виконання процедури шифрування.

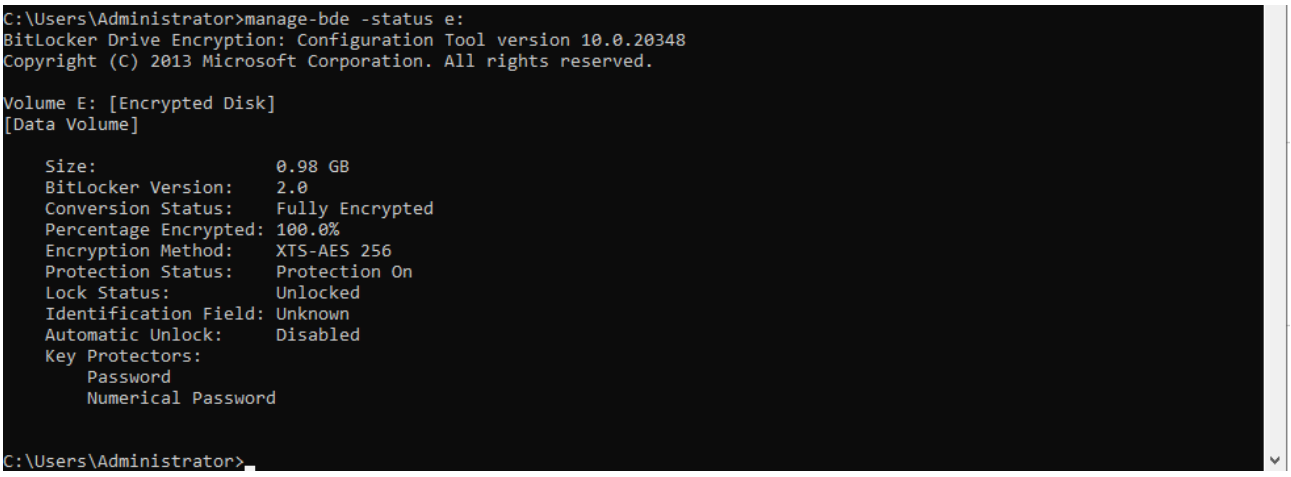

Рисунок 3.11 – Вивід команди `manage-bde -status e:` після виконання шифрування BitLocker в Windows Server 2022

Ці дані вказують, що диск e: повністю зашифровано за допомогою шифрування XTS-AES 256 і захищено паролем. Захист увімкнено, але диск зараз розблоковано, що означає, що він доступний для використання. Автоматичне розблокування вимкнено. Доступ до диска можливий лише після введення пароля.

На рисунку 3.12 показано вікно Active Directory Users and Computers в Windows Server 2022, зокрема інформація про властивості контролера домену PDC.sbtntu.net.

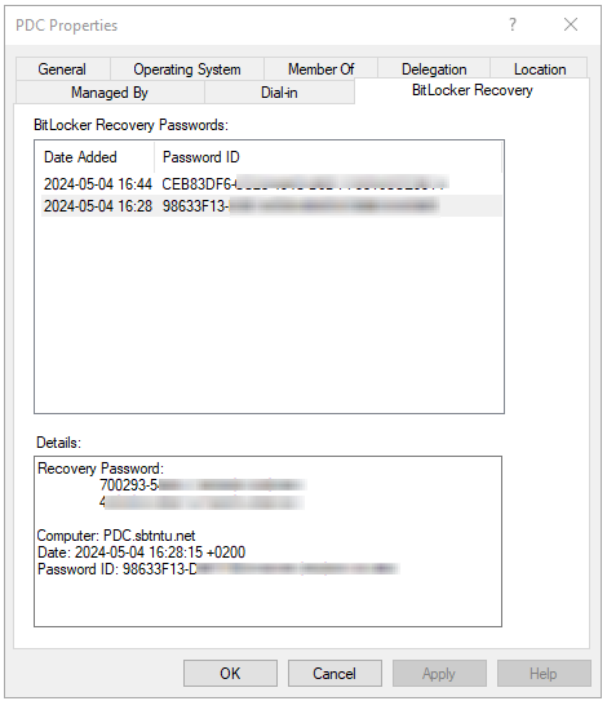

Рисунок 3.12 – Збережені ключі відновлення BitLocker в Active Directory для комп’ютера PDC

Вкладка BitLocker Recovery властивостей об'єкта містить дані про паролі відновлення BitLocker для даного комп'ютера. Ці дані використовуються для управління доступом до зашифрованого диска у випадку, якщо основні методи доступу недоступні або втрачені. Можна побачити, що ключі відновлення зберігаються в Active Directory для забезпечення можливості відновлення у безпечний та організований спосіб. Це важливо для великих організацій, де потрібно мати надійні методи відновлення зашифрованих даних у випадку необхідності.

3.1.3 Шифрування диску в Windows 10 та Windows 11

Виконаємо шифрування системного диску c: в операційній системі Windows 10 за допомогою інструменту manage-bde.

На рисунку 3.13 показано результати виконання команди виводу результатів застосування групових політик в Windows 10.

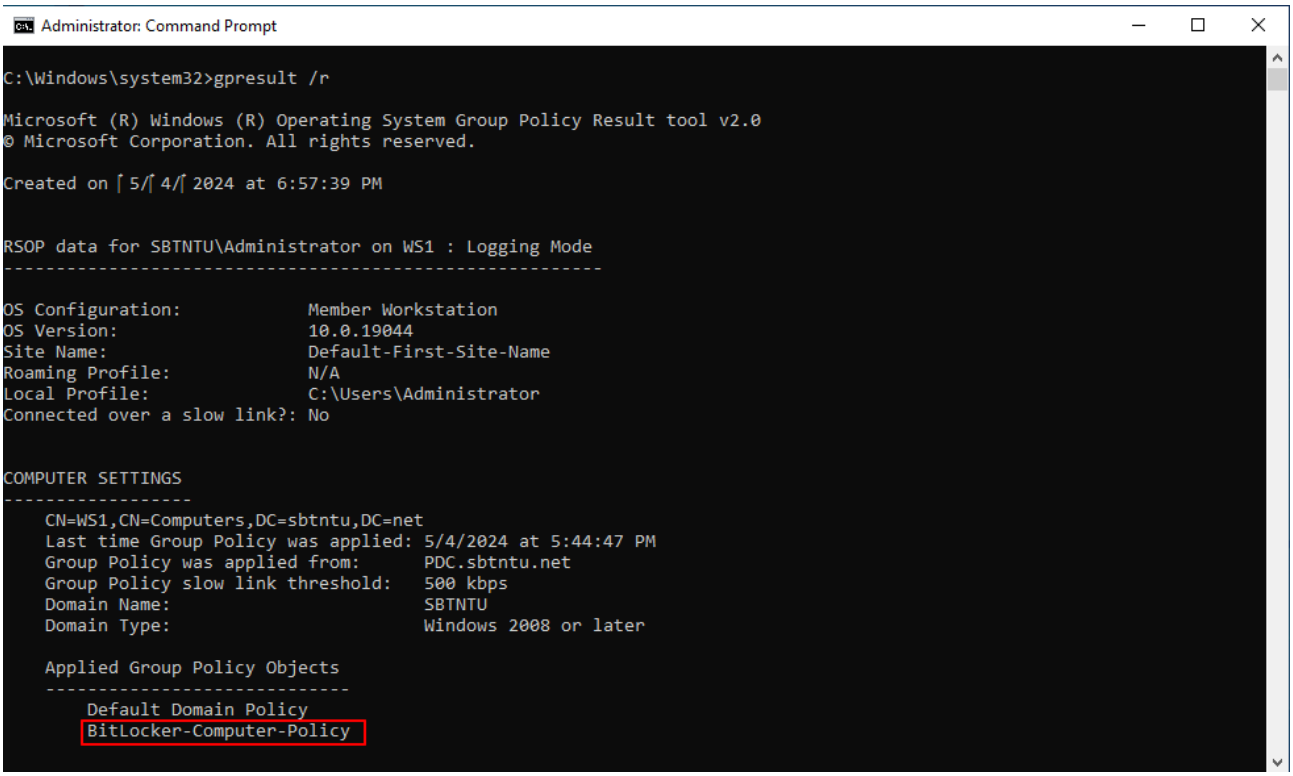

Рисунок 3.13 – Результати виконання команди `gpresult /r` в Windows 10

З рисунку видно, що групова політика BitLocker-Computer-Policy успішно застосована.

На рисунку 3.14 показано вивід команди для перегляду статусу шифрування системного диска за допомогою утиліти manage-bde.

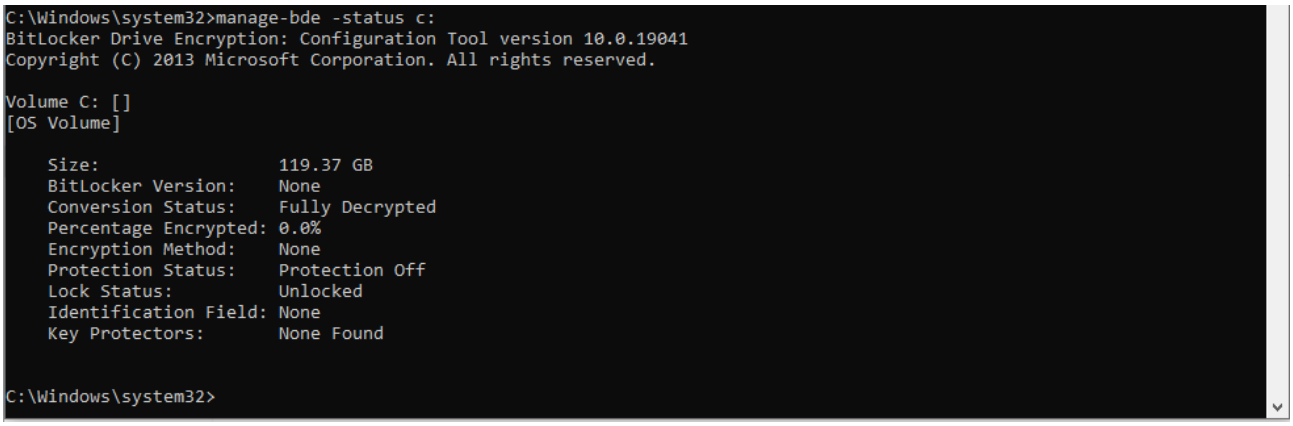

Рисунок 3.14 – Вивід команди `manage-bde -status c:` до запуску процесу шифрування BitLocker в Windows 10

Ці дані вказують, що системний диск c: не зашифровано, шифрування для нього вимкнено, і жодних захисних механізмів для ключів не налаштовано.

На рисунку 3.15 показано вивід команди, яка використовується для додавання ключа відновлення (recovery password) до диску з літерою приводу c:.

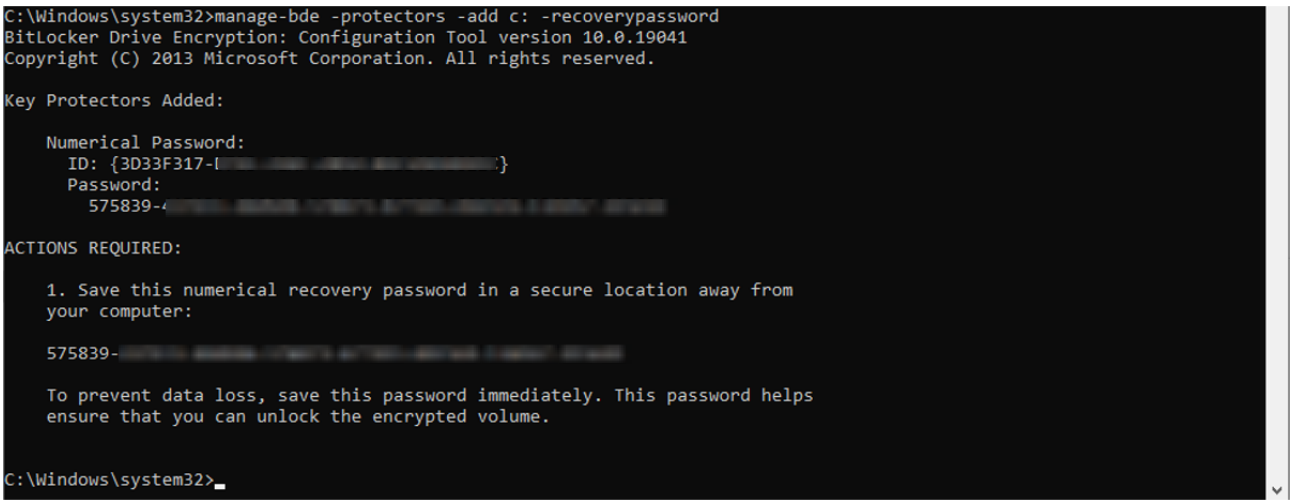

Рисунок 3.15 – Вивід команд додавання ключа відновлення BitLocke в Windows 10

На рисунку 3.16 показано вивід команди увімкнення шифрування BitLocker для системного диску c: за допомогою утиліти manage-bde.

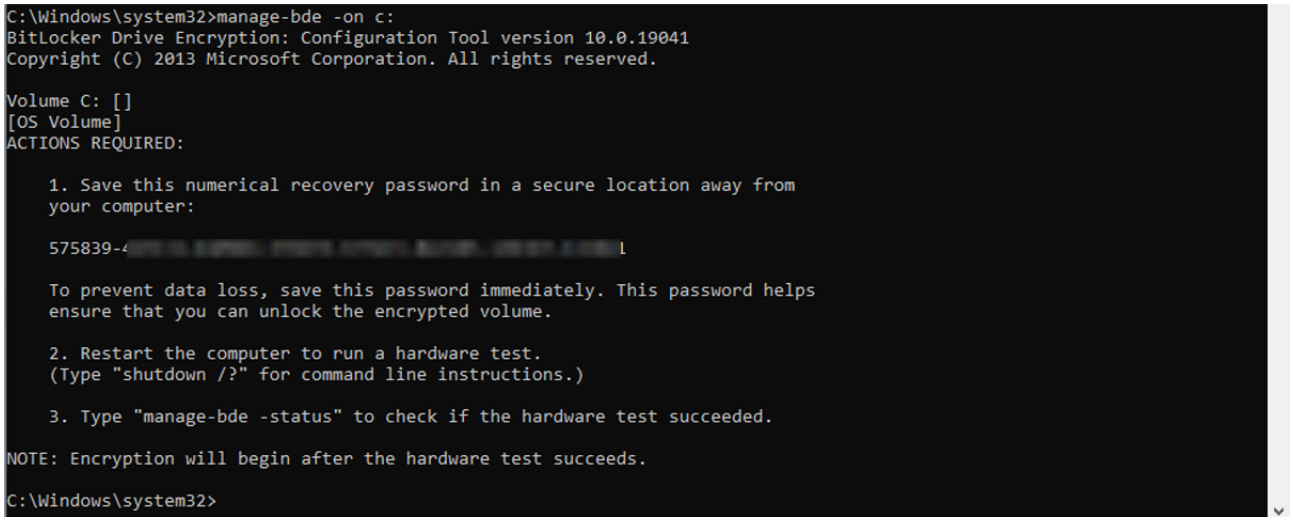

Рисунок 3.16 – Вивід команд увімкнення шифрування BitLocker системного диску в Windows 10

На рисунку 3.17 показано вивід команди, яка додає додатковий метод захисту за допомогою PIN для диска c:.

Рисунок 3.17 – Встановлення додаткового методу захисту за допомогою PIN для диска c: в Windows 10

За допомогою цього методу захисту для доступу до диска потрібно буде ввести як PIN-код, так і використовувати TPM. Такий підхід забезпечує додатковий рівень безпеки, оскільки доступ до даних можливий лише за умови наявності обох факторів автентифікації - TPM та знання PIN-коду.

На рисунку 3.18 показано вивід команди для перегляду статусу шифрування диска c: після виконання процедури шифрування.

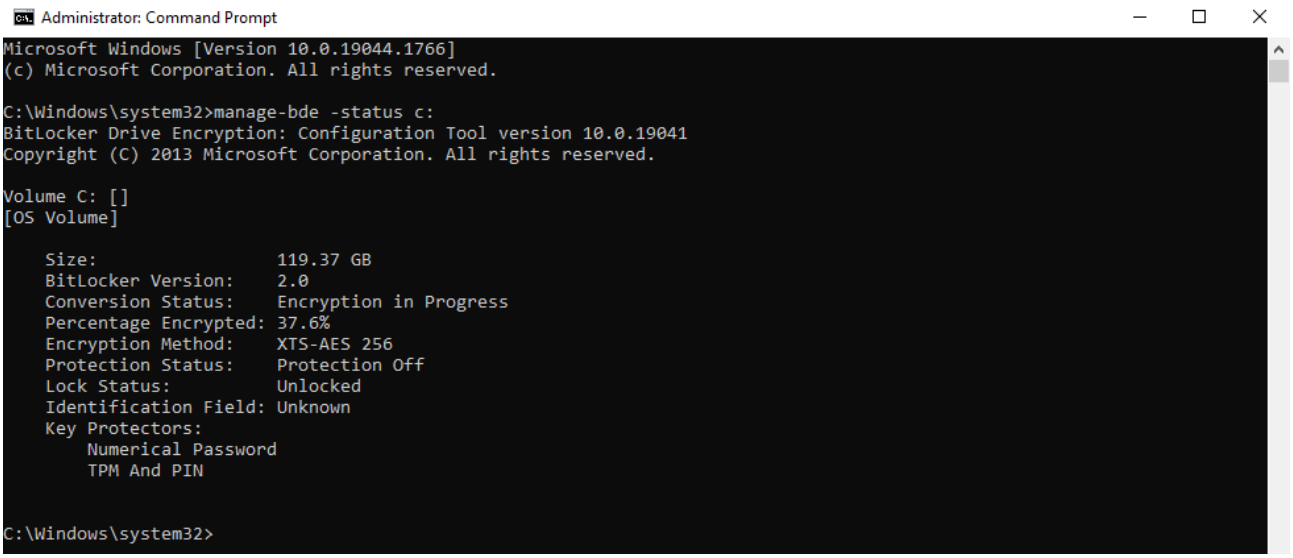

Рисунок 3.18 – Вивід команди `manage-bde -status c:` після виконання шифрування BitLocker в Windows 10

Ці дані вказують, що диск c: зашифровано за допомогою шифрування XTS-AES 256. Диск зараз розблоковано, що означає, що він доступний для використання. Автоматичне розблокування вимкнено. Для доступу до диска використовуються, як TPM так PIN, що забезпечує додатковий рівень безпеки.

На рисунку 3.19 показано вікно Active Directory Users and Computers в Windows Server 2022, зокрема інформація про властивості робочої станції WS1.sbtntu.net.

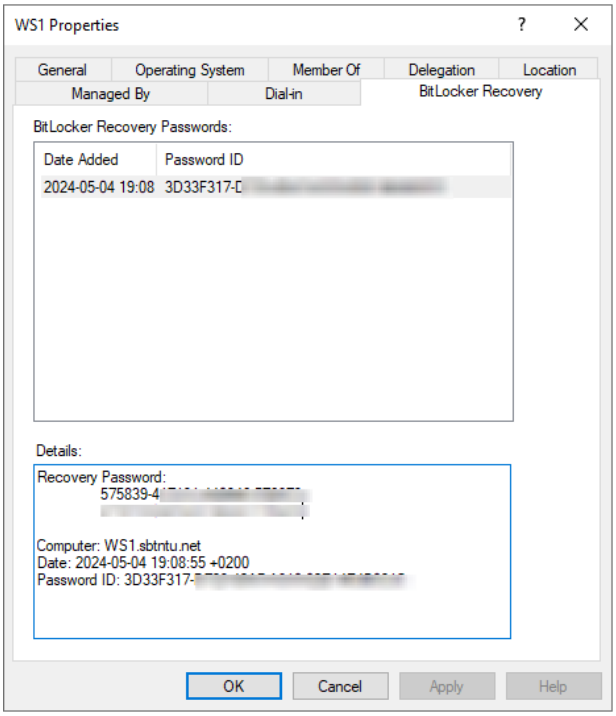

Рисунок 3.19 – Збережені ключі відновлення BitLocker в Active Directory для комп’ютера WS1

Вкладка BitLocker Recovery властивостей об'єкта містить дані про паролі відновлення BitLocker для комп'ютера WS1.

Після завершення шифрування та перевантаження комп'ютера WS1 на початковому етапі завантаження буде виведено екран блокування BitLocker, де потрібно ввести PIN-код, щоб розблокувати системний диск c: (див. рисунок 3.20).

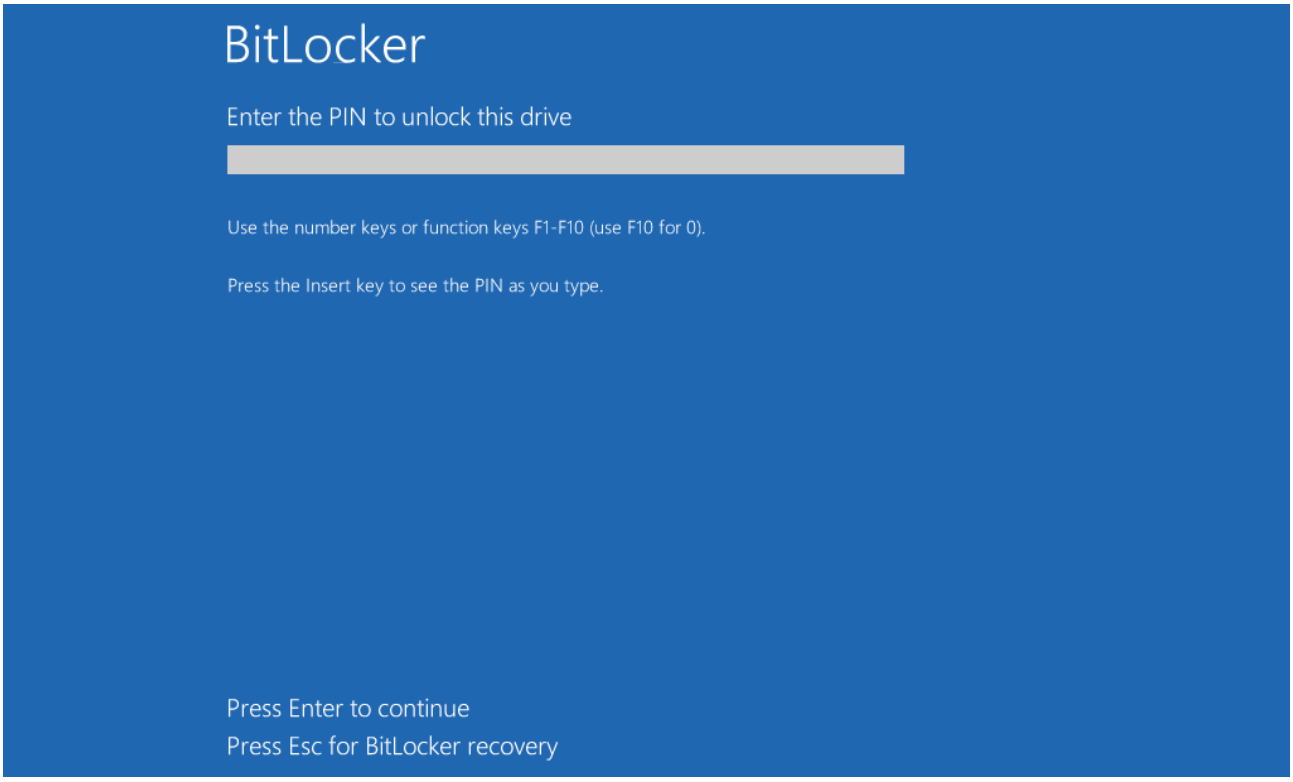

Рисунок 3.20 – Екран блокування BitLocker при старті операційної системи комп’ютера WS1

Цей інтерфейс з'являється при старті системи, коли диск захищений за допомогою BitLocker з використанням PIN як засобу додаткового захисту. Він є частиною заходів безпеки BitLocker, які забезпечують захист даних на диску шляхом їх шифрування і вимагають додаткової автентифікації перед завантаженням системи. Введення правильного PIN-коду дозволить

завантаження операційної системи, в той час як неправильне введення може спричинити виклик опцій відновлення та блокування доступу до системи.

Для підтвердження коректності роботи BitLocker в Windows 11 та можливості автоматичного копіювання ключа відновлення в Active Directory виконаємо шифрування USB диску e: за допомогою інструменту manage-bde.

Послідовність шифрування знімного USB дисків схожа до послідовності шифрування фіксованого диску в операційній системі Windows Server 2022 (див. пункт 3.1.2)

На рисунку 3.21 показано вивід команди для перегляду статусу шифрування диска e: після виконання процедури шифрування.

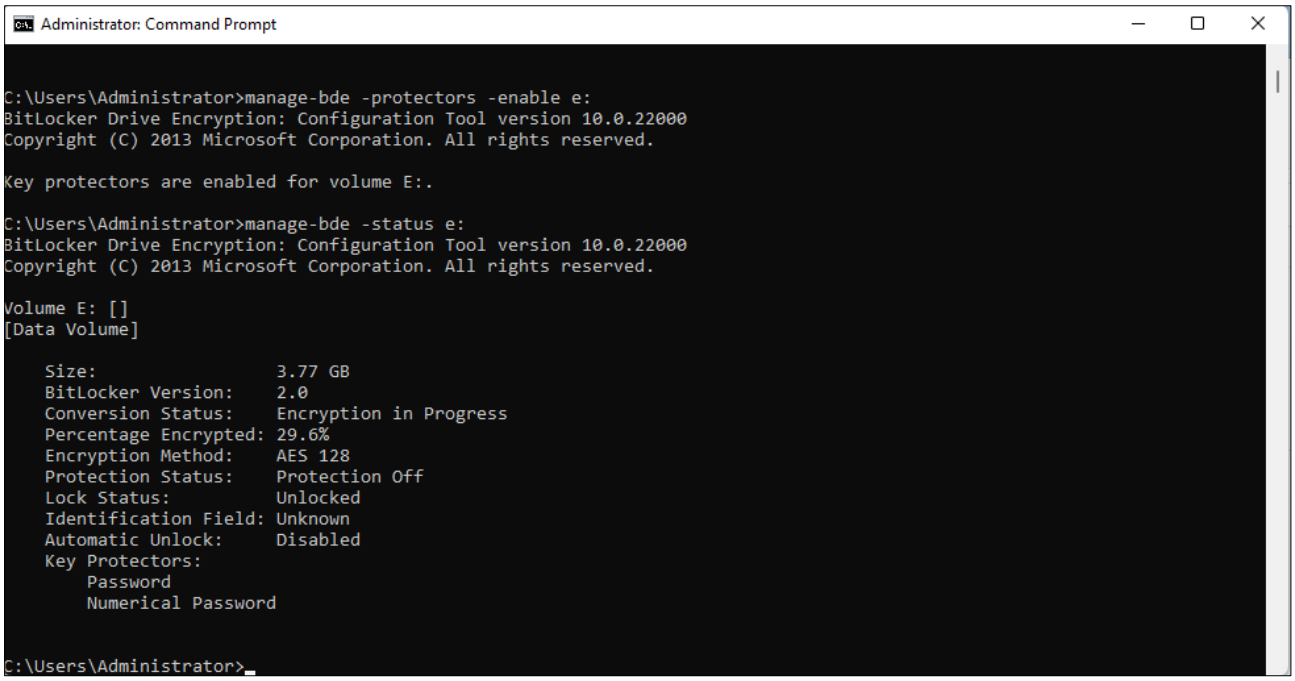

Рисунок 3.21 – Вивід команди `manage-bde -status e:` після виконання шифрування BitLocker в Windows 11

Ці дані вказують, що диск e: зашифровано за допомогою шифрування AES 128 в режимі CBC згідно налаштованої політики шифрування BitLocker (див.рисунок 3.1). Захист увімкнено, але диск зараз розблоковано, що означає, що він доступний для використання. Автоматичне розблокування вимкнено. Доступ до диска можливий лише після введення пароля.

На рисунку 3.22 показано вікно Active Directory Users and Computers в Windows Server 2022, зокрема інформація про властивості робочої станції WS2.sbtntu.net.

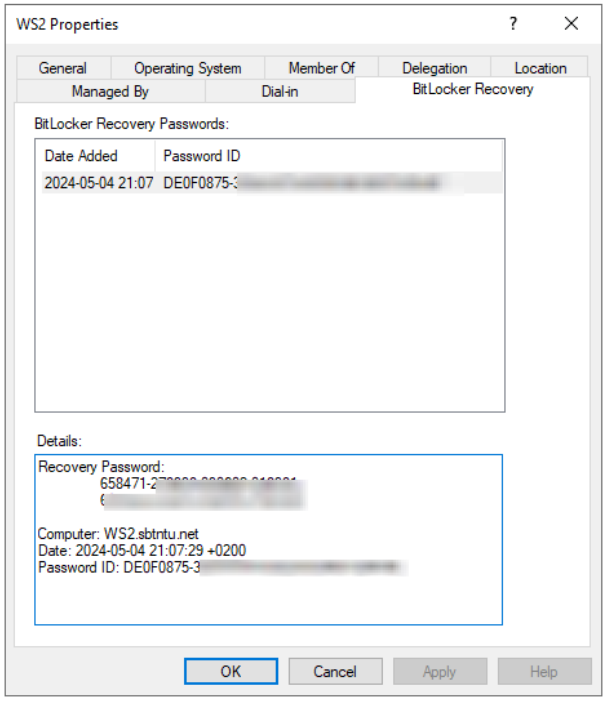

Рисунок 3.22 – Збережені ключі відновлення BitLocker в Active Directory для комп’ютера WS2

Вкладка BitLocker Recovery властивостей об'єкта містить дані про паролі відновлення BitLocker для комп'ютера WS2 з операційною системою Windows11.

3.2 Використання EFS в Active Directory

3.2.1 Налаштування служби сертифікації Active Directory

Служба сертифікації Active Directory (ADCS) - це роль в Windows Server, яка відповідає за видання та управління сертифікатами в рамках інфраструктури відкритих ключів (PKI) [13]. Ці сертифікати використовуються для забезпечення безпеки у протоколах зв'язку та процесах автентифікації.

Цифрові сертифікати можна використовувати для шифрування та цифрового підпису електронних документів і повідомлень, а також для

автентифікації облікових записів комп’ютера, користувача або пристрою в мережі.

Наприклад, цифрові сертифікати використовуються для забезпечення:

- конфіденційності при шифруванні;
- цілісності при цифрових підписах;
- автентифікація шляхом зв’язування ключів сертифіката з обліковими записами комп’ютера, користувача чи пристрою в комп’ютерній мережі.

Кореневі та підпорядковані центри сертифікації (CA) використовуються для видачі сертифікатів користувачам, комп’ютерам і службам, а також для керування дійсністю сертифікатів. Вебреєстрація дозволяє користувачам підключатися до CA за допомогою веббраузера, щоб запитувати сертифікати та отримувати списки відкликаних сертифікатів (CRL). Служба реєстрації мережевих пристроїв дозволяє маршрутизаторам та іншим мережевим пристроям, які не мають облікових записів домену, отримувати сертифікати. Атестація ключа TPM дозволяє центру сертифікації перевірити, чи приватний ключ захищено апаратним TPM і чи CA довіряє TPM. Атестація ключа TPM запобігає експорту сертифіката на неавторизований пристрій і може прив’язати ідентифікатор користувача до пристрою. Вебслужба політики реєстрації сертифікатів дозволяє користувачам і комп’ютерам отримувати інформацію про політику реєстрації сертифікатів. Вебслужба реєстрації сертифікатів дозволяє користувачам і комп’ютерам виконувати реєстрацію сертифікатів через вебслужбу. Разом із вебслужбою політики реєстрації сертифікатів це забезпечує реєстрацію сертифікатів на основі політики, коли клієнтський комп’ютер не є членом домену або коли член домену не підключений до домену.

ADCS використовується для підвищення безпеки шляхом прив’язування ідентифікаційної інформації особи, комп’ютера чи служби до відповідного закритого ключа. ADCS надає економічний, ефективний і безпечний спосіб керування розповсюдженням і використанням сертифікатів. Окрім зв’язування ідентифікаторів і закритих ключів, ADCS також містить функції, які дозволяють керувати реєстрацією та відкликанням сертифікатів. Також є можливість використовувати існуючу ідентифікаційну інформацію кінцевої точки в Active

Directory для реєстрації сертифікатів, тобто є можливість автоматично вставляти інформацію в сертифікати. ADCS також можна використовувати для налаштування групових політик Active Directory, щоб визначити, яким користувачам і машинам дозволено які типи сертифікатів. Конфігурація групової політики дозволяє контролювати доступ на основі ролей або атрибутів.

Програми, які підтримує ADCS, включають захищені/багатоцільові розширення Інтернет-пошти (S/MIME), захищені бездротові мережі, VPN, IPsec, EFS, вхід за допомогою смарт-картки, SSL/TLS і цифрові підписи.

Використання EFS з ADCS забезпечує додаткові можливості керування шифруванням файлів і безпекою даних на рівні організації.

ADCS може виступати як інфраструктура, що надає сертифікати шифрування, які використовуються для захисту ключів EFS. Ці сертифікати видаються для користувачів або комп'ютерів відповідно до правил безпеки, встановлених адміністраторами. ADCS дозволяє централізовано керувати сертифікатами, включаючи їх видачу, відкликання та оновлення. Це спрощує управління сертифікатами, які використовуються для шифрування файлів з EFS.

На рисунку 3.23 показано результати виконання команди PowerShell для встановлення ADCS в Windows Server 2022.

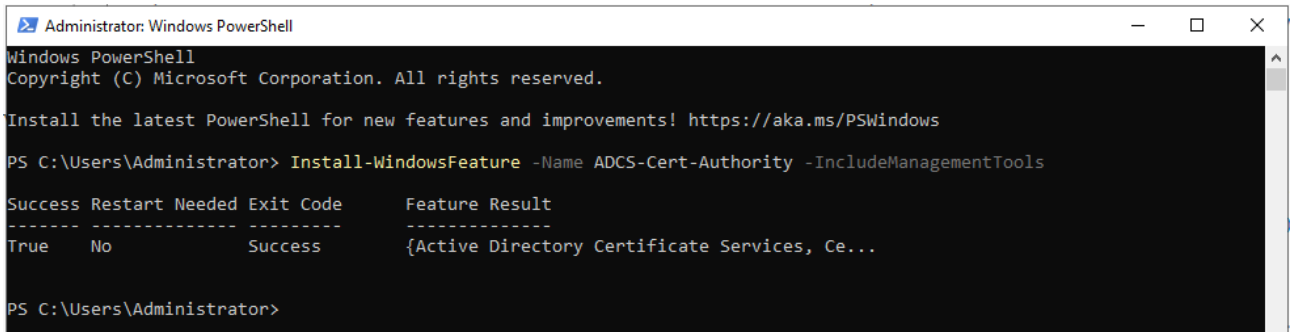

Рисунок 3.23 – Встановлення Active Directory Certificate Services в Windows Server 2022

Команда PowerShell використовується для встановлення ADCS разом з інструментами управління. Результат вказує на те, що встановлення сервісів ADCS пройшло успішно і без необхідності перезапуску системи.

На рисунку 3.24 показано створення конфігурації центру сертифікації (CA) в Windows Server 2022.

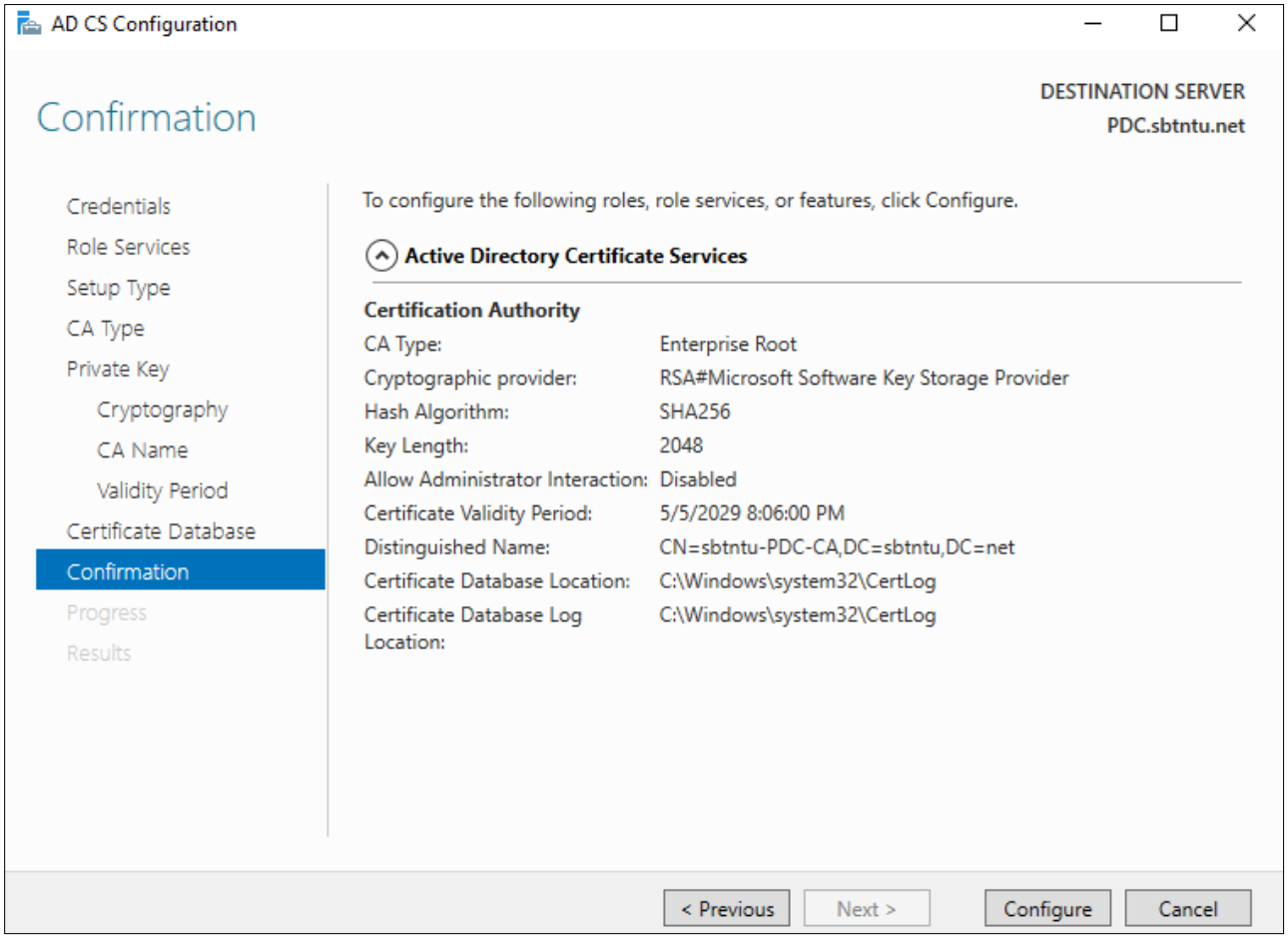

Рисунок 3.24 – Створення конфігурації центру сертифікації в Windows Server 2022

Enterprise Root CA - це кореневий сертифікаційний орган, який випускає кореневі сертифікати і контролює всі підлеглі CA в ієрархії. Криптографічний провайдер RSA/Microsoft Software Key Storage Provider визначає технологію, яка використовується для зберігання та використання криптографічних ключів.

RSA/Microsoft Software KSP є компонентом Windows, що забезпечує зберігання та використання криптографічних ключів. Це один із багатьох провайдерів зберігання ключів, доступних в системах Windows, який дозволяє програмному забезпеченню використовувати криптографічні функції, такі як шифрування, створення цифрових підписів, та управління ключами.

RSA є найпоширеніший алгоритм для створення цифрових підписів і шифрування даних. Microsoft Software KSP підтримує різні довжини ключів RSA, зазвичай від 1024 до 4096 біт, що забезпечує гнучкість у виборі між

безпекою та продуктивністю. Довжина ключа в 2048 біт забезпечує хороший баланс між безпекою та продуктивністю для сучасних криптографічних операцій.

Ключі, що зберігаються за допомогою Microsoft Software KSP, розміщуються у захищеній області системи, яка ізольована від прямого доступу користувачів або програм. Це знижує ризик витоку або компрометації ключів.

Інтеграція Microsoft Software KSP з ADCS дозволяє автоматизувати видачу та управління сертифікатами, забезпечуючи централізоване керування ідентифікаційними даними користувачів.

SHA256 - це алгоритм хешування, який використовується для створення унікального та фіксованого 256-бітного хешу з даних будь-якого розміру.

3.2.2 Шифрування файлі та каталогів в Windows

Для дослідження можливостей EFS для шифрування файлів та каталогів створимо окремий каталог `Data` в Windows Server 2022. Встановимо повний доступ (full control) до даного каталогу для користувачів `testuser1` та `testuser2`. Зробимо даний каталог доступним по мережі та встановимо його, як домашній каталог користувачів `testuser1` та `testuser2` (див. рисунок 3.25).

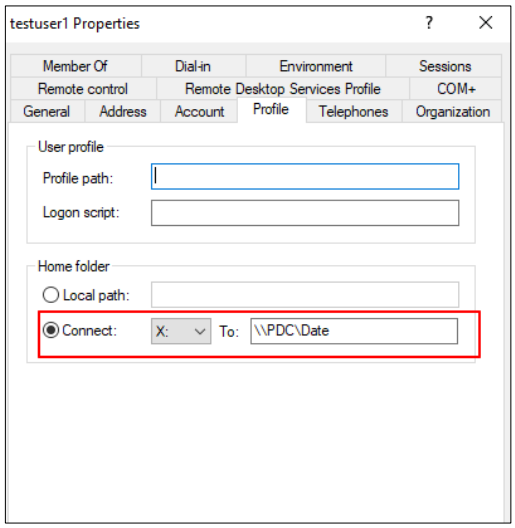

Рисунок 3.25 – Налаштування домашнього каталогу користувача в Windows Server 2022

Домашній каталог вказано, як шлях до мережевого ресурсу `\\PDC\Date`. Це означає, що під час входу в систему для користувачів `testuser1` та `testuser2` буде автоматично під'єднано мережевий диск з вказаним шляхом, де користувачі зможуть зберігати свої файли.

Ця налаштування дозволяє централізувати зберігання даних користувачів на сервері, забезпечувати їх доступність з будь-якого комп'ютера в домені.

Здійснимо вхід в систему на комп’ютері WS1 з логіном `testuser1`. На диску x: створимо тестовий файл `TestEFStestuser1.txt` та виконаємо його шифрування за допомогою EFS (див. рисунок 3.26).

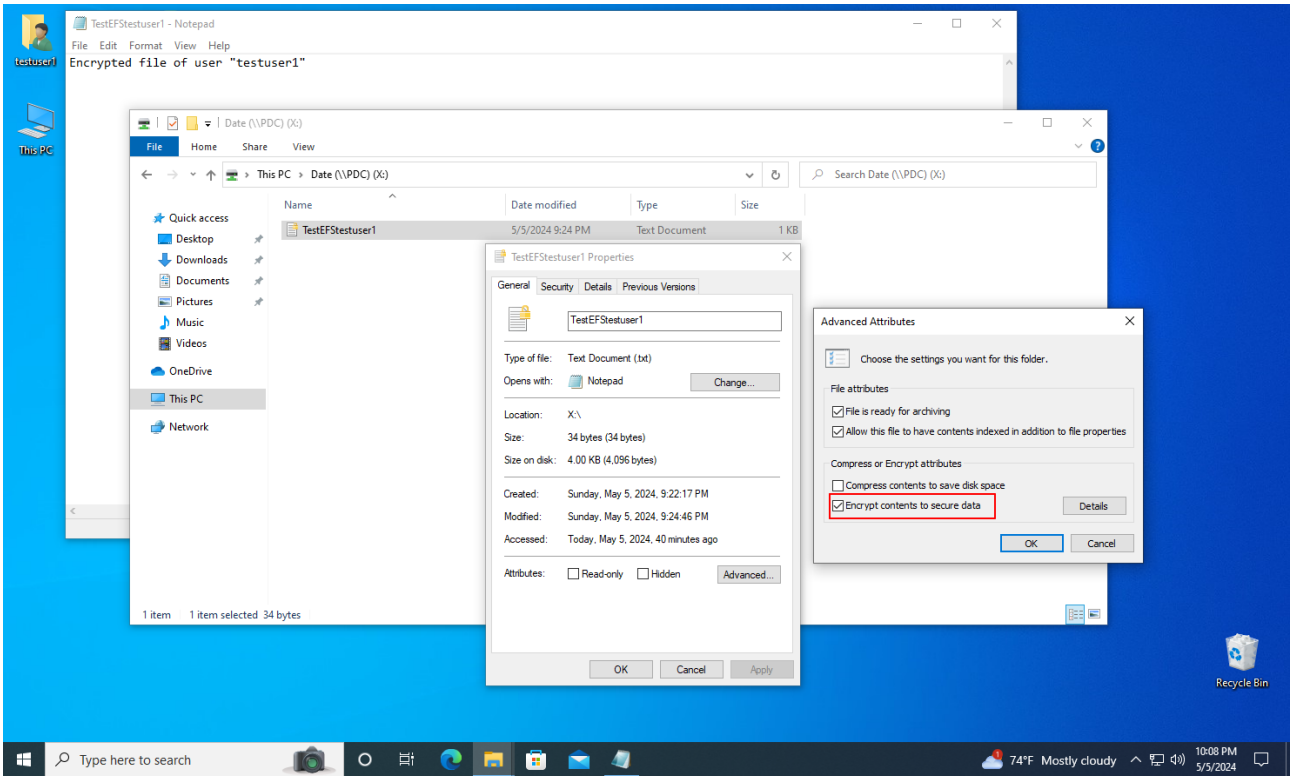

Рисунок 3.26 – Шифрування файлу `TestEFStestuser1.txt` за допомогою EFS в Windows 10

При виконанні шифрування CA видав сертифікат для користувача `testuser1`, який використовуються для захисту ключів EFS.

На рисунку 3.27 показано вікно консолі управління сертифікатами в Windows 10 з секцією особистих сертифікатів користувача `testuser1`.

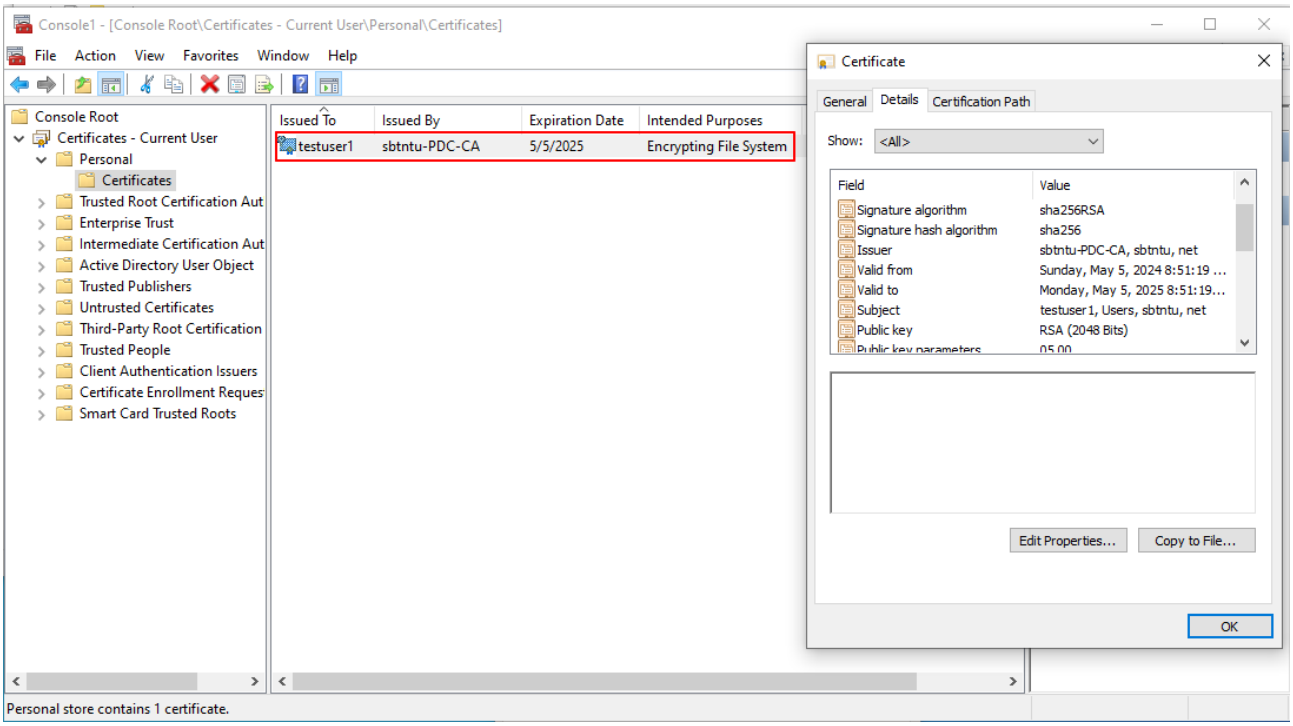

Рисунок 3.27 – Вікно консолі управління сертифікатами в Windows 10

Сертифікат виданий для користувача `testuser1` кореневим центром сертифікації sbtntu-PDC-CA. Цей сертифікат призначений для використання з EFS.

Алгоритм підпису sha256RSA використовує SHA-256 для хешування та RSA для шифрування. Відкритий ключ використовує RSA з довжиною ключа 2048 біт.

Також в консолі управління центром сертифікації в Windows Server 2022 можна також побачити виданий сертифікат для користувача `testuser1` (див. рисунок 3.28).

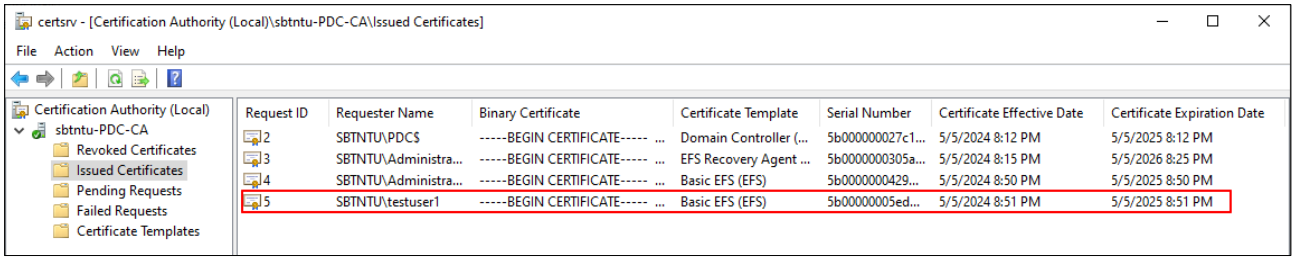

Рисунок 3.28 – Вікно консолі управління CA в Windows Server 2022

Цей інтерфейс дозволяє адміністраторам переглядати деталі сертифікатів, які були видані CA.

Основна представлена інформація:

- `Request ID` - унікальний ідентифікатор запиту на сертифікат.
- `Requester Name` - ім'я користувача або системи, яка зробила запит на сертифікат.
- `Certificate Template` - назва шаблону сертифіката, що був використаний для створення сертифікату.
- `Serial Number` - серійний номер сертифіката, який є унікальним для кожного сертифіката.
- `Certificate Effective Date` - дата, коли сертифікат стає дійсним.
- `Certificate Expiration Date` - дата закінчення терміну дії сертифіката.

Сертифікат, який включає в себе шаблон Basic EFS, використовується для шифрування файлової системи.

Здійснимо вхід в систему на комп’ютері WS1 з логіном `testuser2`. На диску x: можна побачити тестовий файл `TestEFStestuser1.txt`, який зашифрований за допомогою EFS. Користувач має повний доступ до файлу згідно прав доступу файлової системи NTFS (див. рисунок 3.29).

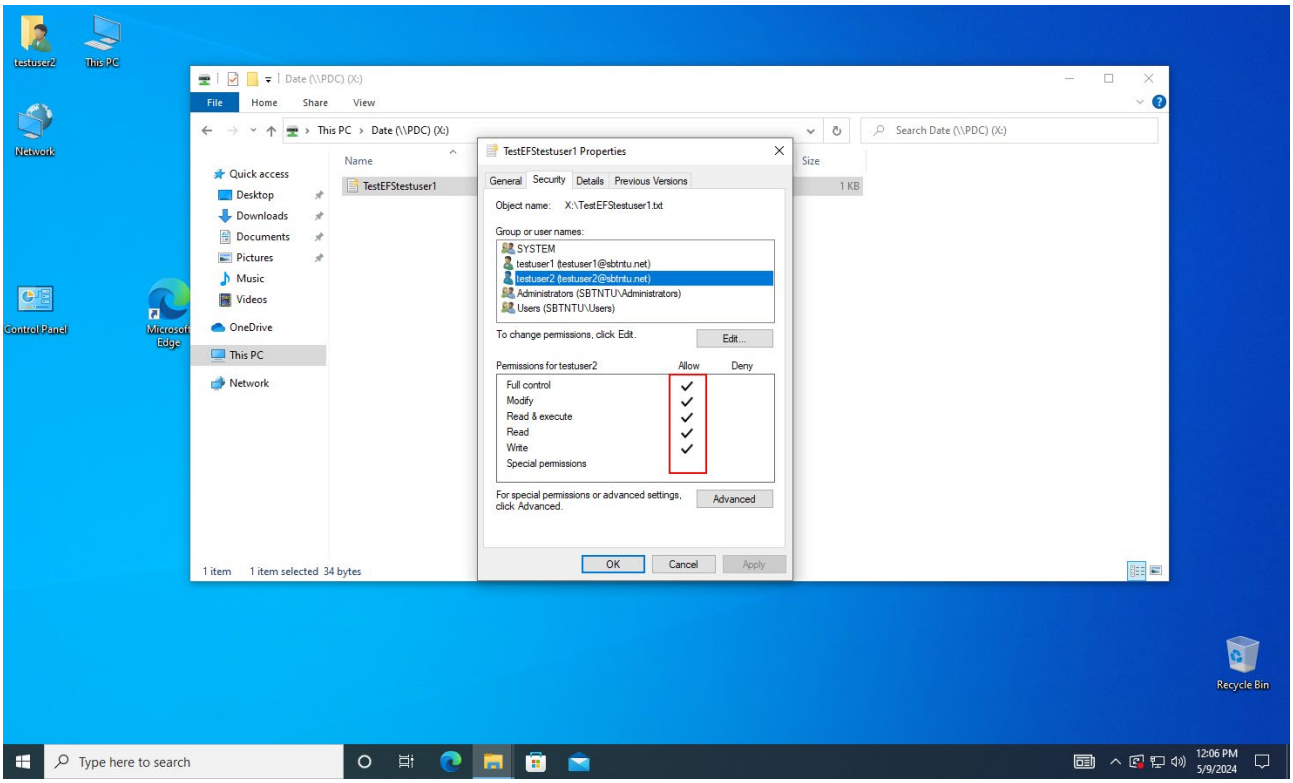

Рисунок 3.29 – Права доступу користувача з логіном `testuser2` до файлу `TestEFStestuser1.txt`

Незважаючи на те що права доступу до файлу `TestEFStestuser1.txt` користувача з логіном `testuser2` дозволяють прочитати вміст файлу про спробі відкрити файл виникає помилка доступу (див. рисунок 3.30).

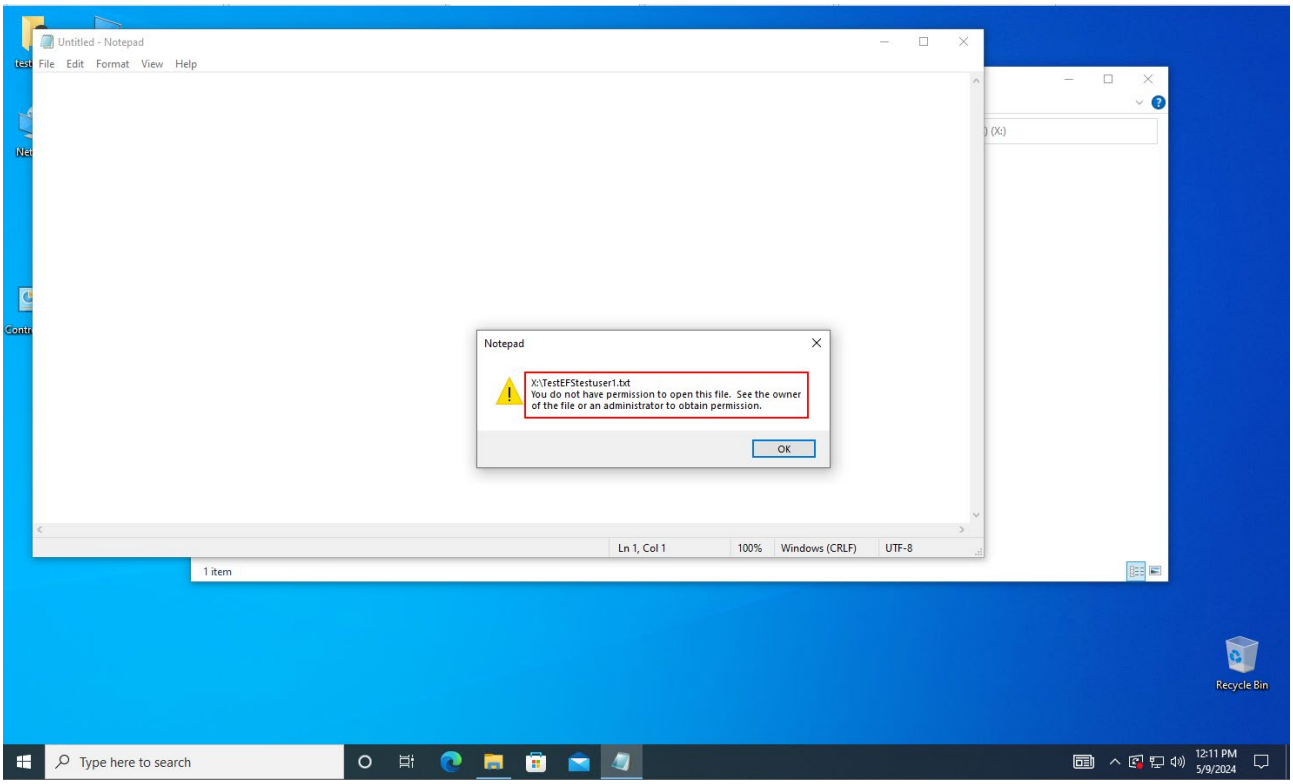

Рисунок 3.30 – Помилка доступу при перегляді файлу `TestEFStestuser1.txt` користувачем з логіном `testuser2`

Файл зашифрований за допомогою EFS. Користувач `testuser2` має права доступу до файлу згідно з налаштуваннями файлової системи NTFS, які дозволяють йому прочитати вміст файлу. Це означає, що на рівні файлової системи користувач має достатні права для доступу до файлу. Незважаючи на наявність прав доступу до файлу на рівні NTFS, для доступу до зашифрованого файлу необхідно мати відповідний сертифікат та ключ для дешифрування. Сертифікат і ключ для EFS зберігаються у профілі користувача, який зашифрував файл. У нашому випадку, файл `TestEFStestuser1.txt` був зашифрований користувачем `testuser1`, і лише користувач `testuser1` або адміністратор з доступом до відповідного сертифікату може розшифрувати цей файл. Адміністратор або користувач `testuser1` може експортувати сертифікат з ключем для дешифрування файлу та надати його користувачу `testuser2` для імпорту у його у профіль. Цей крок дозволять забезпечити доступ користувача `testuser2` до вмісту зашифрованого файлу, якщо це буде необхідно для виконання його обов'язків.

Здійснимо вхід в систему на комп’ютері WS2 з логіном `testuser1`. На диску x: можна побачити тестовий файл `TestEFStestuser1.txt`, який зашифрований за допомогою EFS. Користувач має повний доступ до файлу, оскільки відбувався автоматичний експорт сертифікату користувача з Windows Server 2022 ADCS (див. рисунок 3.31).

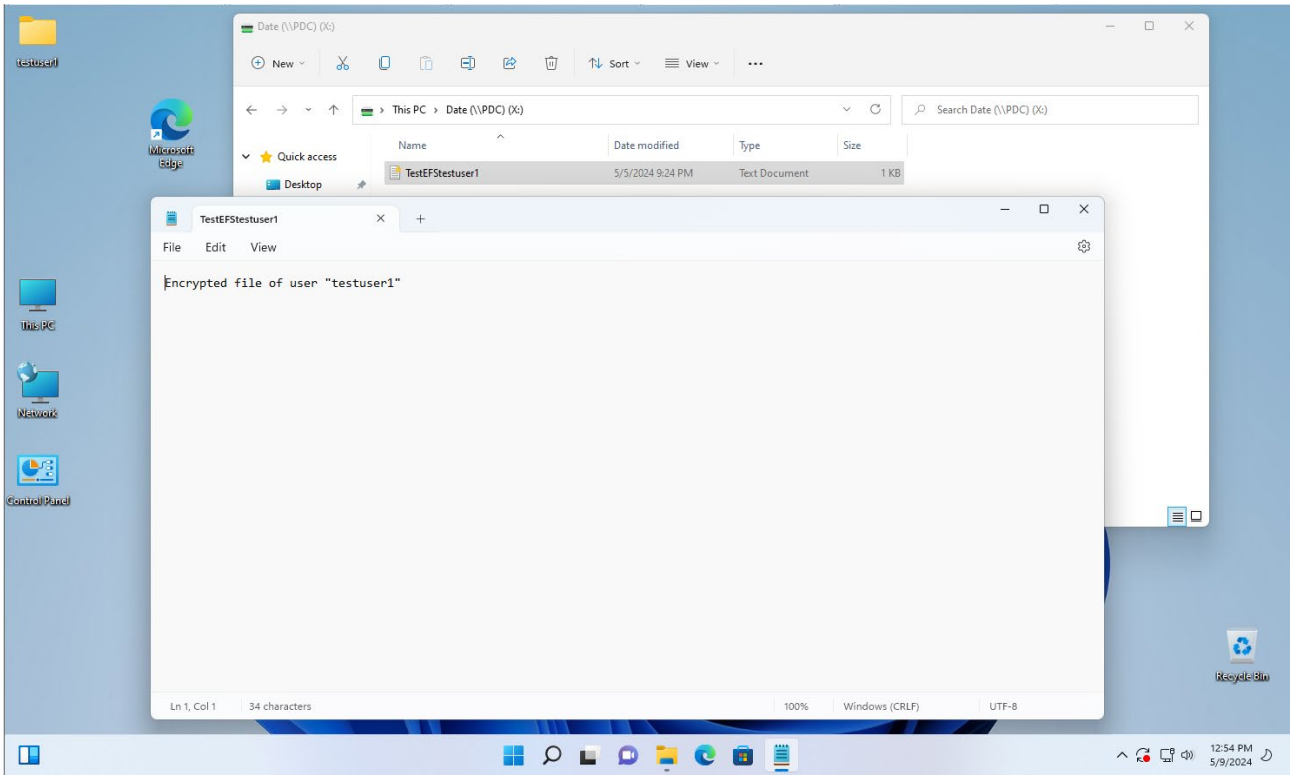

Рисунок 3.31 – Відкриття файлу `TestEFStestuser1.txt` користувачем з логіном `testuser1` на комп’ютері WS2

Користувач з логіном `testuser1` має повний доступ до файлу `TestEFStestuser1.txt`, який зашифрований за допомогою EFS з будь-яких комп’ютерів домену SBTNTU. Це забезпечується службою ADCS з централізованим зберіганням та видачою сертифікатів.

3.3 Висновки до розділу

В третьому розділі було проведено налаштування групові політики в домені так, щоб при використанні BitLocker для шифрування диска автоматично зберігалися ключі відновлення в обліковому записі комп'ютера в Active

Directory. Проведено налаштування алгоритму шифрування та довжини ключа окремо для фіксованих дисків даних, дисків операційної системи XTS-AES 256 та знімних дисків AES-CBC 128. Показано встановлення політики, яка дозволяє налаштувати, додаткову автентифікацію при запуску комп'ютера з або без TPM.

Показано процедури шифрування за допомогою BitLocker та утиліти manage-bde фіксованого диску в операційній системі Windows Server 2022 з використанням додаткового методу захисту за допомогою паролю, системного диску в Windows 10 з використанням додаткового методу захисту за допомогою PIN, USB диску в Windows 11 з використанням додаткового методу захисту за допомогою паролю. Підтверджено коректність зберігання ключів відновлення BitLocker в Active Directory для забезпечення можливості відновлення у безпечний та організований спосіб.

Проведено налаштування служби сертифікації Active Directory (ADCS), яка відповідає за видачу та управління сертифікатами в рамках інфраструктури відкритих ключів (PKI). Показано, що ADCS може виступати як інфраструктура, що надає сертифікати шифрування, які використовуються для захисту ключів EFS. Проведено шифрування файлу за допомогою EFS та показано відповідні сертифікати, які видані CA для користувача. Підтверджено, що користувачі мають повний доступ до своїх зашифрованих за допомогою EFS з будь-яких комп’ютерів домену. Це забезпечується службою ADCS з централізованим зберіганням та видачою сертифікатів при шифрування за допомогою EFS.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Загальні вимоги безпеки з охорони праці для користувачів ПК

Метою даної кваліфікаційної роботи є дослідження методів шифрування даних в стані спокою в ОС Windows Server 2022. Операційні системи встановлюються на серверному обладнанні та персональних комп'ютерах. При роботі з даними системами потрібно забезпечити дотримання вимог з охорони праці, техніки безпеки та протипожежної безпеки при використанні ПК.

Основними регламентуючими нормативними документами охорони праці користувачів комп'ютерів є:

– НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями»;

– ДСанПіН 3.3-2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»;

– НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні».

Вимоги до приміщень, згідно з [15] [16], щодо розташування робочого місця передбачають виконання наступних вимог:

– мінімальна площа, яка виділяється на одне робоче місце повинна становити мінімум 6,0 $м^2$, при об'ємі – мінімум 20,0 $м^3$;

– розташування робочих місць користувачів ПК заборонено у цокольних або підвальних приміщеннях.

При організації робочих місць у НПАОП 0.00-7.15-18 передбачано наявність природного і штучного освітлення. Зазвичай, природне освітлення поступає у приміщення через вікна та світлові прорізи і забезпечує коефіцієнт освітленості на рівні не менше 1,5%. Орієнтація вікон – на північ або північний схід. Штучне освітлення забезпечують відповідні джерела, наприклад, люмінесцентні лампи. Приміщення з комп'ютерною технікою не повинні межувати з будівлями, де рівень шуму чи вібрації перевищує визначені допустимі значення. Покриття підлоги повинне бути матовим з коефіцієнтом відбиття 0,3-0,5. Для внутрішнього оздоблення приміщень слід використовувати

дифузно-відбивні матеріали з коефіцієнтами відбиття для стелі 0,7-0,8, для стін 0,5-0,6 [15].

У приміщеннях, де організовано робочі місця користувачів ПК, повинні бути забезпечені аптечками першої медичної допомоги. Вологе прибирання у таких приміщеннях є обов'язковим кожного дня.

Щодо ергономічної організації робочого місця, то воно також повинно відповідати вимогам, наведеним у [15] [16]. Конструкція робочого місця повинна забезпечити підтримання оптимальної робочої пози. У відповідності до НПАОП 0.00-7.15-18, обладнання і організація робочого місця працюючих з ЕОМ мають забезпечувати відповідність конструкції всіх елементів робочого місця та їх взаємного, розташування ергономічним вимогам з урахуванням характеру і особливостей трудової діяльності.

Висота робочого столу з ПК повинна бути виконана в діапазоні 680...800 мм, а ширина і глибина – 600...1400 мм і 800..1000 мм відповідно. Стіл також повинен мати достатній простір для ніг, що забезпечить зручну осанку користувача. Стілець на робочому місці користувача ПК повинен бути підйомно-поворотним, регульованим за висотою, за кутом і за нахилом сидіння та спинки [14].

Екран комп'ютера повинен бути розміщений на відстані 600...700 мм від очей користувача. Розташування монітору має забезпечувати зручність зорового спостереження у вертикальній площині під кутом +30 градусів до нормальної лінії погляду працівника [15].

Електромережі штепсельних з'єднань та електророзеток для живлення ПК потрібно виконувати за магістральною схемою. При організації робочих місць електромережу штепсельних розеток для живлення ПК у центрі приміщення прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах [15].

Щодо безпеки при роботі з ПК, щодня перед початком роботи необхідно очищати монітор від пилу та інших забруднень. Після закінчення роботи з ПК, він та периферійні пристрої повинні бути відключені від електричної мережі. У разі виникнення певної аварійної ситуації необхідно негайно відключити ПК від

електричної мережі. Не допускається виконувати обслуговування, ремонт та налагодження ПК безпосередньо на робочому місці [15].

Основні вимоги до пожежної безпеки вказані в НАПБ А.01.001-2004 «Правила пожежної безпеки в Україні». Згідно з [15], на та під приміщеннями, в яких розміщені ЕОМ, а також у суміжних із ними приміщеннях не дозволяється розташування приміщень категорій А та Б за вибухопожежною небезпекою.

Фальшпідлога у приміщеннях з ЕОМ має бути з негорючих матеріалів або матеріалів груп горючості Г1, Г2 з межею вогнестійкості не менше 0,5 години. Простір під нею слід розділяти негорючими діафрагмами на відсіки площею не більше 250 м2. Діафрагми повинні мати межу вогнестійкості не менше 0,75 год. Звукопоглинаюче облицювання стін та стель цих приміщень слід виготовляти з негорючих матеріалів або матеріалів груп горючості Г1, Г2. Персональні комп'ютери після закінчення роботи повинні відключатися від мережі. Не рідше одного разу на квартал необхідно очищати від пилу агрегати та вузли, кабельні канали та простір між підлогами [16].

Приміщення повинні бути забезпечені первинними засобами пожежогасіння, а саме вогнегасниками, що використовуються для локалізації і ліквідації пожеж у їх початковій стадії розвитку.

Вогнегасники слід встановлювати у легкодоступних та помітних місцях (коридорах, біля входів або виходів з приміщень тощо), а також у пожежонебезпечних місцях, де найбільш вірогідна поява осередків пожежі. При цьому необхідно забезпечити їх захист від попадання прямих сонячних променів та безпосередньої (без загороджувальних щитків) дії опалювальних та нагрівальних приладів.

Вибір типу та необхідна кількість вогнегасників визначається відповідно до Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 02.04.2004 № 151.

У кваліфікаційній роботі розроблено метод захисту серверів від атак. Дослідження в роботі вимагали взаємодії людини з серверним обладнанням, тому важливим та актуальним було провести аналіз основних вимог до

приміщень та робочих місць з ПК, що дозволило забезпечити комфортні і безпечні умови праці адміністраторів систем.

4.2 Захист людини від впливу іонізуючого випромінювання

Працівники, які виконують роботи з радіоактивними речовинами, повинні перебувати під постійним медичним наглядом, використовувати засоби індивідуального захисту від радіації та прилади індивідуального дозиметричного контролю (універсальні радіометри) для своєчасного виявлення і вимірювання рівня випромінювання [17].

Захищаючись від зовнішнього іонізуючого опромінювання при роботах із закритими джерелами випромінювання, тобто такими, які виключають можливість потрапляння радіоактивних речовин у навколишнє середовище, перш за все необхідно не допустити переопромінення працівників.

Основним способами захисту від цього є:

- зменшення активності джерела, з яким контактують працівники під час конкретного технологічного процесу – досягається шляхом використання речовин із меншою активністю;

- зменшення часу контакту з джерелом випромінювання – досягається шляхом вдосконалення організації робіт і технологічного виробничого процесу та проведення попередніх тренінгів працівників;

- збільшення відстані між людиною і джерелом – використовується, як правило, при контакті з точковим джерелом випромінювання шляхом використання дистанційних універсальних маніпуляторів та інших автоматизованих пристроїв;

- розташування між людиною і джерелом захисного екрану (стаціонарного, пересувного, розбірного, настільного тощо), тобто пристрою, який зменшує інтенсивність випромінювання до безпечного рівня [17].

Для виготовлення екранів, а також для захисту працівників в стаціонарних спорудах, використовується бетон, чавун, сталь, алюміній, скло, свинець та інші матеріали. Від дії рентгенівських променів застосовують екрани зі сталевого

листа товщиною 0,5-1 мм або алюмінію товщиною 3 мм, спеціальної гуми. Оглядові вікна виконують з плексигласу товщиною 30 мм або з покритого оловом скла товщиною 9 мм.

Для захисту шкіри від забруднень радіоактивними речовинами та запобігання їх попаданню всередину організму, захисту від альфа і бета-випромінювання передусім застосовуються засоби індивідуального захисту (ЗІЗ) від радіації.

Отже, засоби захисту від радіації використовуються у тих випадках, коли інші заходи недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення.

З урахуванням зазначеного прогнозу на території області може виникнути складна радіаційна обстановка наслідки якої вимагатимуть від органів виконавчої влади, органів місцевого самоврядування, суб'єктів господарювання, на які покладено виконання завдань щодо захисту населення і територій від надзвичайних ситуацій, оперативного реагування та дій [17].

Місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання здійснюють для забезпечення захисту людей від впливу іонізуючих випромінювань наступні заходи:

- приймають згідно з законодавством України рішення щодо застосування на підвідомчій території заходів втручання у разі радіаційних аварій;

- організовують проведення в установленому порядку щорічні обстеження з метою оцінки стану захисту людини від впливу іонізуючих випромінювань та ведення екологічного паспорта підвідомчої території;

- здійснюють організаційне керівництво системою обліку та контролю доз опромінення населення на підвідомчій території;

- організовують контроль за виконанням заходів щодо захисту людини від впливу радіонуклідів, що містяться у будівельних матеріалах;

- затверджують відповідні плани щодо захисту населення від радіаційних аварій та їх наслідків;

- забезпечують постійну готовність засобів оповіщення населення на підвідомчій території про виникнення радіаційної аварії;

- організовують контроль за виконанням заходів щодо захисту населення від радіаційних аварій та їх наслідків;

- забезпечують населення, в місцях його проживання, інформацією щодо рівнів опромінення людини та заходів захисту від впливу іонізуючих випромінювань, що виконуються на підвідомчій території;

- розроблюють та впроваджують програми захисту людей від впливу іонізуючих випромінювання;

- здійснюють оповіщення населення у разі виникнення радіаційної аварії та інформування про рятувальні та профілактичні заходи у зв’язку з цим.

Для виконання вищезазначених заходів залучаються органи управління, сили і засоби обласної територіальної та функціональних підсистем єдиної державної системи цивільного захисту (далі – ЄДС ЦЗ), порядок дій яких визначено Планом реагування на надзвичайні ситуації, пов'язаних з викидом радіоактивних речовин.

Режими захисту робітників і службовців на суб'єктах господарювання вводяться в дію рішенням керівників об'єктів. Незалежно від місця розміщення суб'єкту господарювання (в населеному пункті або за його межами) на його території вводиться в дію свій режим захисту з урахуванням рівнів радіації, виміряних на об'єкті, і реального ступеню захисту працівників і службовців.

При виникненні комунальної радіаційної аварії окрім термінових робіт щодо стабілізації радіаційного стану (включаючи відновлення контролю над джерелом) місцеві органи виконавчої влади, органи місцевого самоврядування, суб'єкти господарювання одночасно здійснюють заходи, спрямовані на:

- зведення до мінімуму кількості осіб з населення, які зазнають аварійного опромінення;

- запобігання чи зниження індивідуальних і колективних доз опромінення населення;

- запобігання чи зниження рівнів радіоактивного забруднення продуктів харчування, питної води, сільськогосподарської сировини і сільгоспугідь, об'єктів довкілля (повітря, води, ґрунту, рослин тощо), а також будівель і споруд.

Для населення, робітників та службовців суб'єктів господарювання, які можуть потрапити в зону випадіння радіоактивних опадів, доцільно завчасно, виходячи з конкретних місцевих умов, розрахувати варіанти режимів радіаційного захисту [18].

З урахуванням вищезазначеного, режими радіаційного захисту вводяться в дію місцевими органами виконавчої влади, органами місцевого самоврядування, суб'єктами господарювання з метою захисту людей від впливу іонізуючого випромінювання у разі загрози або виникнення надзвичайних ситуацій, пов'язаних з радіаційними аваріями.

ВИСНОВКИ

В процесі написання кваліфікаційної роботи було проаналізовано та показано практичну реалізацію вбудованих методів шифрування даних в стані спокою в операційній системі Windows з акцентом на централізоване управління з використання можливостей Windows Server 2022 ADDS.

У першому розділі було здійснено аналіз різних станів, в яких можуть перебувати дані. Було розглянуто дані у спокійному стані, дані у русі та дані в процесі використання. Також було здіснено огляд заходів захисту даних для кожного з цих станів, таких як застосування протоколу TLS та шифрованого VPN для захисту даних у русі, використання MFA та SSO для захисту даних, шо використовуються, а також використання шифрування для захисту даних у стані спокою. Також в розділі було детально розглянуто алгоритми шифрування даних у стані спокою. Визначено, що симетричне блокове шифрування є основним методом для цього. Був проведений аналіз та наведено характеристики основних симетричних блокових шифрів, таких як AES, DES, 3DES, Blowfish, Serpent, Twofish та Camellia.

У другому розділі була розроблена лабораторна схема середовища для дослідження методів шифрування даних в стані спокою в операційній системі Windows з акцентом на централізоване управління з використання можливостей Windows Server 2022 ADDS. Встановлено та налаштовано Windows Server 2022 з роллю ADDS. Також встановлено та налаштовано робочі станції з Windows 10 та Windows 11. Здійснено приєднання Windows 10 та Windows 11 до домену.

Було описано вбудовані методи шифрування даних в операційній системі Windows, зокрема можливості BitLocker та EFS. BitLocker дозволяє шифрувати всі дані на жорсткому диску або обраних томах, тоді як EFS шифрує файли та папки на рівні файлової системи. Підкреслено переваги застосування BitLocker з TPM, що гарантує найвищий рівень захисту для пристроїв під управлінням Windows. Описано режими шифрування даних за допомогою BitLocker з використанням симетричних шифрів AES-CBC 128, AES-CBC 256, XTS-AES 128 та XTS-AES 256. Описано принцип роботи EFS в Windows. Показано, що EFS

використовує симетричне шифрування AES для шифрування файлів та асиметричне шифрування RSA для захисту ключів шифрування.

У третьому розділі було налаштовано групові політики в домені так, щоб автоматично зберігалися ключі відновлення в обліковому записі комп'ютера в Active Directory при використанні BitLocker для шифрування диска. Також було встановлено алгоритм шифрування та довжину ключа окремо для фіксованих дисків даних, дисків операційної системи (XTS-AES 256) та знімних дисків (AES-CBC 128). Налаштовано політику, що дозволяє налаштувати додаткову автентифікацію при запуску комп'ютера з або без TPM.

Продемонстровано процедури шифрування за допомогою BitLocker та утиліти manage-bde фіксованого диску в операційній системі Windows Server 2022 з використанням додаткового методу захисту за допомогою паролю. Також показано шифрування системного диску в Windows 10 з використанням додаткового методу захисту за допомогою PIN та USB-диску в Windows 11 з використанням додаткового методу захисту за допомогою паролю.

Проведено налаштування служби сертифікації Active Directory (ADCS), яка відповідає за видачу та управління сертифікатами в рамках інфраструктури відкритих ключів (PKI). Показано, що ADCS може виступати як інфраструктура, що надає сертифікати шифрування, які використовуються для захисту ключів EFS. Проведено шифрування файлу за допомогою EFS та показано відповідні сертифікати, які видані CA для користувача.

У результаті проведеного аналізу було встановлено, що шифрування даних у стані спокою є важливим заходом для захисту конфіденційної інформації під час зберігання і неактивного використання. Це допомагає запобігти ризику втрати даних або несанкціонованого доступу до них.

У результаті проведення тестування було підтверджено коректність зберігання ключів відновлення BitLocker в Active Directory для забезпечення можливості відновлення у безпечний та організований спосіб. Підтверджено, що з використанням службою ADCS з централізованим зберіганням та видачою сертифікатів для шифрування за допомогою EFS користувачі мають повний доступ до своїх зашифрованих файлів з будь-яких комп’ютерів домену.

Дослідження та практична реалізація підтвердили ефективність та надійність вбудованих методів шифрування даних в стані спокою в операційній системі Windows з централізованим управління за допомогою Active Directory Domain Services на базі Windows Server 2022.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Types of Encryption for in Motion, in Use, at Rest Data URL: https://cyscale.com/blog/types-of-encryption/ (дата звернення: 09.05.2024).

2. VPN security: How VPNs help secure data and control access. URL: https://www.cloudflare.com/learning/access-management/vpn-security/ (дата звернення: 09.05.2024).

3. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми Україна), 191-193.

4. What Are the Different Types of VPN? URL: https://www.paloaltonetworks.com/cyberpedia/types-of-vpn (дата звернення: 09.05.2024).

5. Стебельський, М., & Букатка, С. (2023). Загальносистемні криптографічні політики ОС Linux. Порівняльний аналіз. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 177-178.

6. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. In Journal of Physics: Conference Series (Vol. 1840, No. 1, p. 012026). IOP Publishing.

7. DES vs 3DES vs Blowfish vs AES URL: https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes (дата звернення: 09.05.2024).

8. Active Directory Domain Services Overview URL: https://learn.microsoft.com/uk-ua/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 09.05.2024).

9. Тимощук, В., & Стебельський, М. (2023). Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 183-184.

10. BitLocker overview URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/ (дата звернення: 09.05.2024).

11. Using Encrypting File System URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb457116(v=technet.10)?redirectedfrom=MSDN (дата звернення: 09.05.2024).

12. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06. 2024; Луцьк Україна), 266-267.

13. Kharchenko, A., Halay, I., Zagorodna, N., & Bodnarchuk, I. (2015). Trade-off optimal decision of the problem of software system architecture choice. In Proceedings of the International Conference on Computer Sciences and Information Technologies, CSIT 2015 (pp. 198-205)

14. What is Active Directory Certificate Services? URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview (дата звернення: 09.05.2024).

15. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями. Київ. 2018.

16. Катренко Л.А., Катренко А.В. Охорона праці в галузі комп’ютинґу. Львів: Магнолія-2006. 2012. 544 с.

17. Желібо Є. П., Сагайдак І. С. Безпека життєдіяльності. Навчальний посібник для аудиторної та практичної роботи. К.:ЕКОМЕН. 2011. 200 с.

18. Депутат О. П., Коваленко І. В., Мужик І. С. Цивільна оборона. Навчальний посібник. За редакцією полковника В.С. Франчука. Львів: Афіша. 2000. 336 с.