МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Комплексна кваліфікаційна робота бакалавра

ІНФОРМАЦІЙНА СИСТЕМА З ОРГАНІЗАЦІЇ МЕРЕЖЕВОГО ДОСТУПУ КАФЕДРИ ІТ. АДМІНІСТРУВАННЯ СЕРВЕРНОЇ ЧАСТИНИ, НАЛАШТУВАННЯ ПОЛІТИК ДОСТУПУ ТА БЕЗПЕКИ

Здобувач освіти гр. ІНз-81С Дмитро ЦИПЛІН

Науковий керівник,
кандидат технічних наук, доцент,
завідувач кафедри інформаційних технологій Віра ШЕНДРИК

Завідувач кафедри
доктор технічних наук, професор Анатолій ДОВБИШ

Суми 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

Затверджую_____
Зав. кафедри Довбиш А.С.
"_____" _____20__р.

ЗАВДАННЯ

до комплексної кваліфікаційної роботи

здобувача вищої освіти за освітньо-професійною програмою «Інформатика» спеціальності 122 «Комп'ютерні науки» другого (бакалаврського) рівня заочної форми навчання групи ІНз-81С Ципліна Дмитра Олександровича

Тема: «ІНФОРМАЦІЙНА СИСТЕМА З ОРГАНІЗАЦІЇ МЕРЕЖЕВОГО ДОСТУПУ КАФЕДРИ ІТ. АДМІНІСТРУВАННЯ СЕРВЕРНОЇ ЧАСТИНИ, НАЛАШТУВАННЯ ПОЛІТИК ДОСТУПУ ТА БЕЗПЕКИ»

Затверджена наказом по СумДУ
№_____ от _____20__р.

Зміст пояснювальної записки: 1) аналіз проблеми та постановка задачі; 2) вибір методів розв'язання задачі; 3) розробка інформаційного і програмного забезпечення

Дата видачі завдання «_____» _____ 20__ р.
Керівник роботи _____ Віра ШЕНДРИК
Завдання прийняв до виконання _____ Дмитро ЦИПЛІН

РЕФЕРАТ

Записка: 32 стор., 16 рис., 1 табл., 1 додаток, 19 джерел.

Об’єкт дослідження — процес проєктування інформаційної системи з організації мережевого доступу випускової кафедри закладу вищої освіти.

Мета роботи — розробка інформаційної системи з організації мережевого доступу випускової кафедри закладу вищої освіти.

Методи дослідження — методи аналізу і інформаційного синтезу інформаційних систем, методи проєктування, налаштування та тестування комп’ютерних мереж.

Результати — розроблено інформаційної системи з організації мережевого доступу випускової кафедри ІТ спрямування закладу вищої освіти. При цьому запропоновано комплекс інформаційного, алгоритмічного та програмного забезпечення основних компонентів таких систем з урахуванням особливостей організації мережевого доступу в Сумському державному університеті. Основну увагу дослідження приділено автоматизації процесів налаштування і тестування комп’ютерної мережі і її окремих компонентів. Програмна реалізація інформаційної системи виконана з використанням мови програмування C#.

МОДЕЛЬ МЕРЕЖЕВОГО ДОСТУПУ, КОМП’ЮТЕРНА МЕРЕЖА,
ГРУПОВІ ПОЛІТИКИ

ЗМІСТ

ВСТУП

Інформаційні технології є невід’ємною частиною сучасного світу, вони значною мірою визначають подальший економічний та суспільний розвиток людства. У цих умовах революційних змін вимагає й система навчання. Звідси можна сказати, що актуальність даного питання має місце у сучасному освітньому середовищі, адже нині якісне викладання дисциплін не може здійснюватися без використання засобів і можливостей, які надають комп’ютерні технології та Інтернет. Інформаційні технології, ІТ – сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів. Технології, що забезпечують та підтримують інформаційні процеси, тобто процеси пошуку, збору, передачі, збереження, накопичення, тиражування інформації та процедури доступу до неї. Інформаційно-комунікаційні технології (ІКТ, від англ. Information and communications technology, ICT) – часто використовується як синонім до інформаційних технологій (ІТ), хоча ІКТ це загальніший термін, який підкреслює роль уніфікованих технологій та інтеграцію телекомунікацій (мережевих та бездротових з'єднань), комп'ютерів, підпрограмного забезпечення, програмного забезпечення, накопичувальних та аудіовізуальних систем, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ складається з ІТ, а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу.

1 ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ ОГЛЯД

1.1 Сучасні інформаційно-комунікаційні технології організації мережевого доступу

Ресурси локальної мережі - це все, чим володіють об'єднані в мережу комп'ютери. Мережеві ресурси можна розділити на три групи:

− апаратні ресурси – це периферійні пристрої комп'ютерів (сканери, принтери та ін.);

− інформаційні ресурси - мережеві диски, папки, документи;

− програмні ресурси - встановлені програми.

У невеликих локальних мережах всі комп'ютери за своїми мережевими функціями можуть бути рівними. Користувачі можуть самостійно вирішувати, які ресурси свого комп'ютера зробити загальнодоступними. З кожного мережевого комп'ютера користувач також може отримати доступ до загальних ресурсів інших користувачів. Такі мережі називаються однорангові. Однак у великих мережах з великим числом комп'ютерів доцільно виділяти один або декілька потужних комп'ютерів для обслуговування потреб мережі. Такі окремі потужні комп'ютери називають серверами. Як сервер зазвичай використовується потужний комп'ютер з великим об’ємом оперативного записуючого пристрою, жорсткими дисками великої ємності, високою тактовою частотою та великою кількістю ядер процесорів. Всі інші комп'ютери називаються клієнтами або робочими станціями. Мережі з виділеним сервером називають дворанговими, хоча частіше можна зустріти вказівку «мережа типу клієнт-сервер». Робота таких мереж будується на основі чіткого розподілу функцій клієнтів і серверів.

Функції клієнта:

− надання користувачам інтерфейсу для формування запитів до мережевого ресурса;

− відправка запитів серверу;

− отримання відповідей від сервера, інтерпретація і подання користувачеві в потрібній формі.

Функції сервера:

− отримання від клієнтів запитів до мережевого ресурса;

− з'ясування доступу клієнта на виконання конкретного запиту;

− виконання запитів згідно повноважень і доступу клієнтів:

− відправка клієнтам результатів.

І на сервері, і на клієнті повинна бути встановлена мережева операційна система. Операційні системи на клієнті і сервері не обов’язково мають бути однаковими. Можуть бути відмінними за функціями модифікації однієї операційної системи. Крім того, на сервері встановлюються спеціальні серверні ролі для виконання специфічних функцій: наприклад, роль маршрутизатора для доступу в мережу Інтернет, або роль поштового сервера для управління електронною поштою і календарем клієнтів. А на комп'ютерах-клієнтах інсталюються відповідні клієнтські додатки: браузер Google Chrome для виходу в мережу Інтернет або програма MS Office Outlook для синхронізації з електронною поштовою скринькою. До основних функцій мережевих ОС відносять:

− управління файлами та каталогами;

− авторизацію клієнта та захист від несанкціонованого доступу;

− забезпечення відмовостійкості інформації.

Управління каталогами та файлами в мережах полягає в забезпеченні доступу до даних, які розташовані в інших вузлах мережі. При обміні інформацією забезпечується необхідний рівень конфіденційності.

Засоби захисту можуть дозволяти доступ до певних даних тільки з обраних клієнтів, в обумовлений час, певну кількість раз, тощо. У кожного користувача можуть бути свої права доступу з обмеженням доступних каталогів або ожливих дій, наприклад, заборона зміни вмісту деяких каталогів або файлів.

Відмовостійкість забезпечується встановленням для серверів автономних або дублюючих джерел живлення, резервного копіювання інформації на дискових накопичувачах, тощо. Обов’язкова наявність у системі

двох копій даних, розташованих на різних жорстких дисках. Очевидно, що дублювання це надійних захист інформаційних ресурсів.

Найбільшого поширення в даний час набули мережеві ОС двох сімейств: UNIX (FreeBSD, Linux та ін.) і Windows (Windows Server, Windows 10, Windows 11), та, зважаючи на потреби кафедри ІТ і нормативні документу СумДУ, ми використовуємо тільки операційні системи сімейства Windows.

1.2 Постановка задачі

Результати проведеного аналітичного огляду доводять актуальність практичної задачі розробки інформаційної системи з організації мережевого доступу випускової кафедри ІТ спрямування закладу вищої освіти. Метою кваліфікаційної роботи бакалавра є проєктування і реалізація такої системи для кафедри інформаційних технологій Сумського державного університету (далі – СумДУ).

При цьому основні завдання роботи включають:

1) Розміщення необхідних серверів, підключених до загальної мережі СумДУ.

2) Налаштування вищезазначених серверів згідно з потребами користувачів (співробітників, викладачів та студентів).

3) Організація мережевого програмно-апаратного сховища для збереження інформації.

4) Забезпечення резервного копіювання інформації.

5) Перевірка працездатності інформаційної системи з організації мережевого доступу.

2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ОРГАНІЗАЦІЇ МЕРЕЖЕВОГО ДОСТУПУ

2.1 Вимоги до інформаційно-телекомунікаційної системи

Проведено аналіз нормативних документів та спроєктовано інформаційну систему згідно з корпоративними політиками роботи та мережевого доступу до інформаційних ресурсів Сумського державного університету. Відповідно до «Положення про Центр телекомунікаційних технологій та комп'ютерного забезпечення», на базі СумДУ створено єдину інформаційно-телекомунікаційну систему (далі-ІТС). Дана ІТС передбачає:

1. Забезпечення проведення узагальненого аналізу стану використання комп'ютерної техніки та периферійного обладнання університету;
2. Забезпечення централізованого антивірусного захисту локальних комп'ютерів, серверів університету;
3. Відповідно до замовлень загальноуніверситетських структурних підрозділів та у відповідності до планів роботи Центру, забезпечення встановлення, оновлення ліцензійного програмного забезпечення (далі-ПЗ) загального, наукового призначення, здійснення консультативної підтримки системних адміністраторів структурних підрозділів інститутів/факультетів щодо встановлення ПЗ;
4. Адміністрування, технічне обслуговування, інсталяція та системне супроводження головних серверів, які забезпечують роботу телекомунікаційної мережі університету;

З усього вище викладеного, модель мережевого доступу розроблено на базі нормативних документів СумДУ.

2.2 Модель мережевого доступу

Модель доступу є важливою складовою інтегрованої в інформаційно-комунікаційне середовище кафедри ІТ системи захисту інформації. Розглянемо типову архітектуру даної системи в цілому з зазначенням місця і ролі моделі доступу в кожному з її складових.

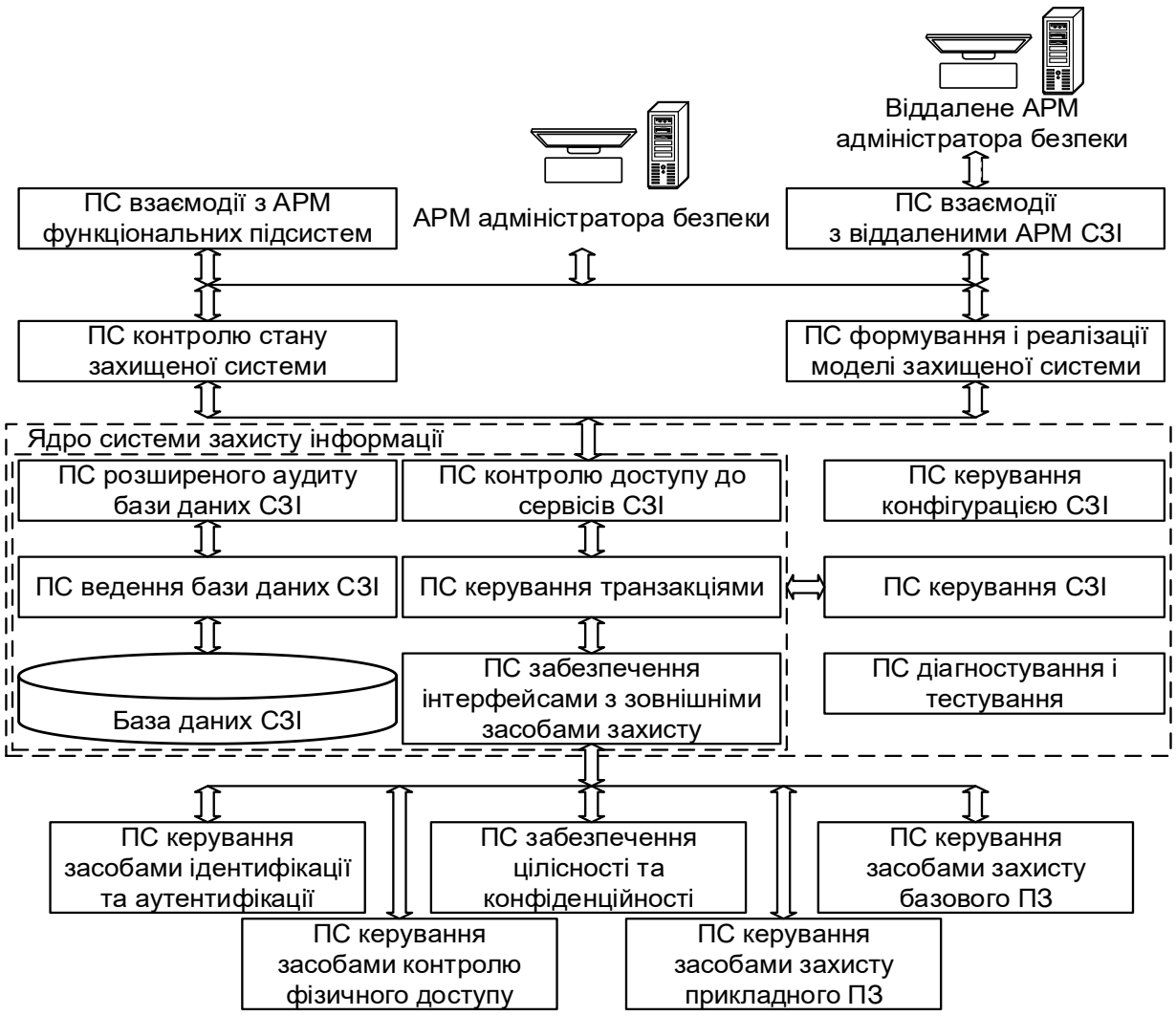

Рисунок 1.1 – Архітектура інформаційної системи мережевого доступу

У цій системі для реалізації функцій керування базовими сервісами безпеки використовують такі підсистеми (ПС):

ПС керування засобами ідентифікації і аутентифікації, що забезпечує керування сервісами ідентифікації і аутентифікації, які реалізовані в СЗІ, включаючи засоби ідентифікації і аутентифікації базового або прикладного програмного забезпечення (ПЗ);

ПС забезпечення цілісності і конфіденційності, що реалізує функції: управління доступом до ресурсів інформаційної системи, керування сервісами контролю і відновлення цілісності, а також криптографічних перетворень;

ПС керування засобами захисту базового ПЗ, що реалізує функції: інтерпретації команд СЗІ в команди керування засобами захисту базового ПЗ, прийому і обробки повідомлень про події від засобів захисту базового ПЗ;

ПС керування засобами захисту прикладного ПЗ, що реалізує функції: інтерпретації команд СЗІ в команди керування засобами захисту прикладного ПЗ, прийому і обробки повідомлень про події від засобів захисту прикладного ПЗ;

ПС керування засобами контролю фізичного доступу, що реалізує функції: інтерпретації команд СЗІ в команди керування засобами контролю фізичного доступу, прийому і обробки повідомлень від засобів контролю фізичного доступу.

Для координації взаємодії різних підсистем у складі СЗІ використовуються такі підсистеми:

ПС контролю доступу до сервісів СЗІ, що реалізує функції генерації сеансових ключів при підключенні до сервера СЗІ, контролю повноважень адміністраторів на виконання команд керування процесом захисту і ведення бази даних (БД) повноважень адміністраторів[1];

ПС керування транзакціями, що реалізує функції підтримки транзакційної моделі виконання команд СЗІ, а саме команда вважається виконаною, якщо виконані всі складові її операції; в іншому випадку система повинна бути повернута в початковий стан;

ПС ведення бази даних СЗІ, що реалізує функції: інтерпретації команд СЗІ в команди керування даними; підтримки ефективного функціонування БД СЗІ; резервування та відновлення БД СЗІ після збоїв;

ПС розширеного аудиту бази даних СЗІ, що реалізує функції: візуальної побудови і виконання складних запитів по БД СЗІ (аудит моделі системи, аудит журналу подій); подання результатів запитів в зручній для адміністратора формі, аналіз БД СЗІ з метою виявлення «вузьких» місць в захисті або спроб несанкціонованого доступу[2];

ПС забезпечення інтерфейсів із зовнішніми засобами захисту, що реалізує функції: встановлення зв'язку з активними підсистемами керування засобами контролю фізичного доступу, засобами контролю цілісності і криптографічного захисту, засобами захисту базового і прикладного ПЗ; надання сервісів відповідної підсистеми керування в залежності від команди, яка була отримана від підсистеми формування і реалізації моделі захищеної системи;

ПС керування СЗІ, що реалізує функції керування і контролю за функціонуванням ядра СЗІ;

підсистема керування конфігурацією СЗІ, що реалізує функцію ведення внутрішньої БД, яка визначає поточну структуру активних засобів захисту, правил розмежування доступу до ресурсів СЗІ, налаштування параметрів функціонування інших підсистем СЗІ;

ПС діагностики і тестування, що забезпечує: контроль (і при необхідності, відновлення) цілісності програмних засобів СЗІ, локалізацію помилок при збоях і відмовах; тестування і діагностику при старті системи, при відновленні після збоїв і за запитом адміністратора безпеки[3].

Для централізованого керування захищеною системою за допомогою адміністраторів безпеки СЗІ використовуються:

автоматизоване робоче місце (АРМ) адміністратора СЗІ, де реалізуються функції: надання графічного інтерфейсу; видачі візуальних або звукових попереджень про події, що мають критичний вплив на безпеку системи;

ПС взаємодії з віддаленими АРМ, що реалізує функції: надання сервісів СЗІ для віддаленого використання; захисту інформації між СЗІ і віддаленим АРМ (в тому числі з використанням криптографічних методів);

ПС взаємодії з АРМ функціональних підсистем, що реалізує функцію керування потоком інформації між СЗІ та АРМ функціональних підсистем (АРМ адміністратора БД, АРМ адміністратора програмно-технічного комплексу, АРМ адміністратора телекомунікацій і мереж);

ПС контролю стану захищеної системи, що реалізує функції: ведення журналу подій; відстеження і обробки критичних подій; надання засобів керування правилами відстеження подій для окремих підсистем[4];

ПС формування і реалізації моделі захищеної системи, що реалізує функції: автоматизованого формування моделі захищеної системи, тобто створення структури об'єктів захисту, суб'єктів інформаційної діяльності та правил розмежування доступу для захищеної системи; ведення класифікаторів типів об'єктів, суб'єктів, режимів доступу і повноважень суб'єктів; ведення класифікаторів подій.

Зауважимо, що, функції керування СЗІ реалізують політику безпеки, а саме: керують сервісами безпеки, координують їх взаємодію, здійснюють контроль функціонування захищеної інформаційної системи. Забезпечення і контроль безпеки - це комбінація технічних і адміністративних заходів[5]. Адміністратор безпеки витрачає більше 60% свого робочого часу на технічну роботу, пов'язану з керуванням програмами та іншими засобами контролю доступу, захистом портів тощо, і тільки 40% йде на вирішення адміністративних завдань (розробку документів, пов'язаних із захистом ІБ, процедур перевірки системи захисту тощо) [6]. Збільшення кількості робочих станцій і використання програмних засобів, що включають велику кількість різноманітних компонентів, - все це призводить до такої ситуації, коли адміністратор безпеки вже фізично виявляється не в змозі оперативно аналізувати величезний обсяг відомостей, що містяться в журналі реєстрації подій СЗІ[7]. Це особливо важливо в умовах, коли на порядок денний ставиться завдання реалізації попереджувальної стратегії захисту, у відповідності до якої необхідно забезпечити необхідний рівень захищеності ІС в умовах впливу на неї не тільки вже відомих (тобто таких, що проявлялися в ІС раніше) або найбільш небезпечних загроз, а й від усіх потенційно можливих (в тому числі апріорно невідомих) загроз ІС.

3 ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

3.1 Вибір засобів програмної реалізації системи

Система побудована за допомогою програмних засобів на базі ОС Windows Server 2016. Судячи з поставленої задачі, нам необхідно використовувати наступні функції в роботі кафедри ІТ:

− Аутентифікацію та перевірку доступу до інформації бере на себе система Microsoft Active Directory (далі - MS AD). Означена система обрана на підставі інтеграції з існуючою системою СумДУ. Таким чином ми гарантуємо надійність, швидкість, відмовостійкість та захищеність роботи з інформацією в локальній мережі. Використовуємо також можливості журналів вдалої або невдалої авторизації. Обмеження використання мережевих дисків та доступу до загальних ресурсів реалізовано за допомогою GPO (Group Policy Object) [8].

− Функцію налаштування клієнтської частини ПЗ бере на себе система MS Endpoint Configuration Manager Current Branch. Така система дозволяє одночасно розповсюджувати еталонні образи ОС для швидкого налаштування комп’ютерів за допомогою локальної мережі. Організовано можливість розповсюдження програмного забезпечення, заздалегідь погодженого адміністраторами. Таким чином кожен користувач може встановити або видалити необхідне програмне забезпечення без участі адміністратора та без ризику для локальної мережі, інформації тощо[9].

− Функцію оновлення програмного забезпечення виконує система WSUS (MS Windows System Update Service), за допомогою якої виконується централізоване завантаження, перевірка та розповсюдження оновлень ОС, програмного забезпечення, драйверів пристроїв, тощо[10].

− Автоматизоване встановлення програмного забезпечення з антивірусного захисту реалізуємо за допомогою того ж MS Endpoint Configuration Manager Current Branch[11]. Дана система дозволяє централізовано керувати антивірусним захистом та своєчасним оновленням вірусних сигнатур.

− Активацію корпоративних ліцензій програмних продуктів компанії Microsoft реалізовано за допомогою системи MS Key Management Services (KMS) [12].

− Дані користувачів зберігаються на мережевому сховищі HP StoreEasy 1430 під управлінням ОС Windows 2019 Server Storage. Організацію доступу до ресурсів налаштовано за допомогою групових політик MS AD з використанням груп користувачів. Мережеві диски, відповідно означених груп, монтуються під час авторизації користувача на клієнтській операційній системі[13].

3.2 Короткий опис програмної реалізації

3.2.1 Сервіси MS Active Directory

На сервері під керуванням ОС MS Windows Server 2016 додаємо роль «Доменні служби Active Directory» [15]. Також автоматично буде встановлено обов’язкову роль «DNS сервер». Після встановлення ролей буде запропоновано провести перше налаштування служби AD:

1. У вікні Майстер налаштування доменних служб обираємо опцію Додати новий домен в існуючий ліс. Існуючий ліс має ім’я – SSU.LOCALNET. Нове ім’я обираємо – IT.
2. Обираємо ім’я нового домену (буде створено піддомен існуючого домену, тобто IT.SSU.LOCALNET).
3. Лишаємо всі опції за замовченням та підтверджуємо встановлення.

Виконуємо налаштування користувачів, груп та групових політик:

1. На контролері домену відкриваємо консоль Active directory – користувачі та комп’ютери.
2. Створюємо новий підрозділ Кафедра IT, в якому також створюємо підрозділи згідно нумерації аудиторій на кафедрі (рис. 3.1) [16].

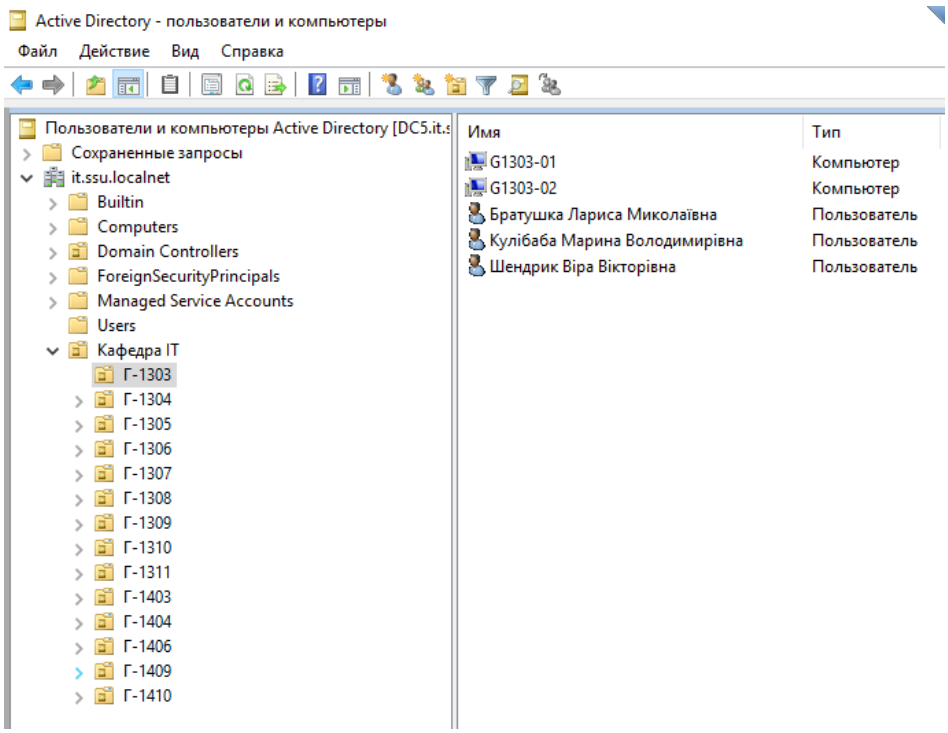

Рисунок 3.1 – Створення нового підрозділу Кафедра IT в Active directory

3. Створюємо об’єкти користувачів та групи користувачів (рис. 3.2).

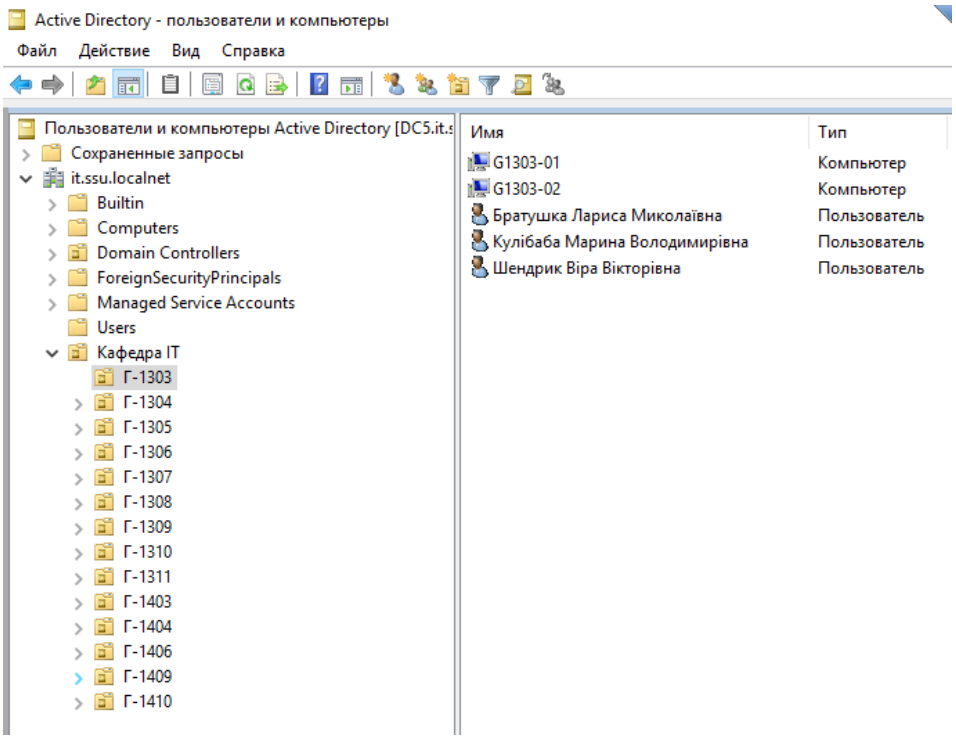

Рисунок 3.2 – Створення об’єктів користувачів

Додаємо користувачів у відповідні групи, згідно планів доступу до інформаційних ресурсів (приклад – рис. 3.3).

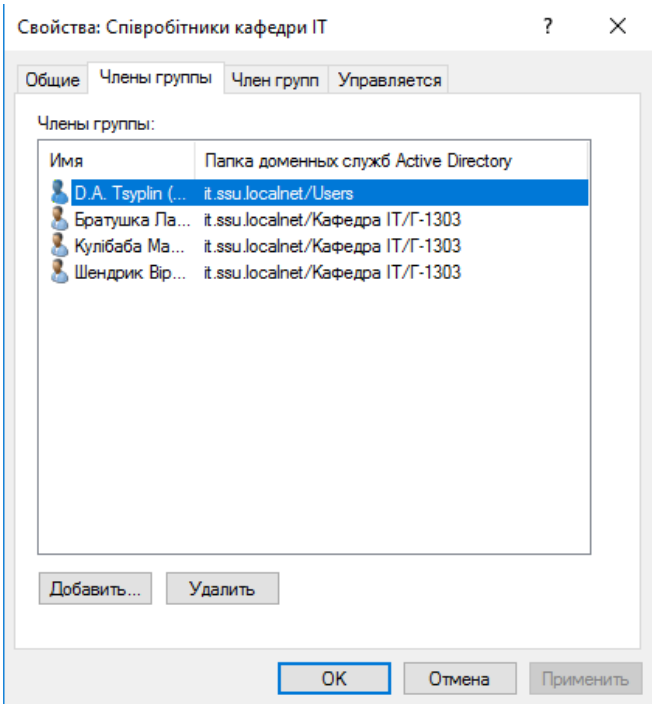

Рисунок 3.3 – Створення груп користувачів

4. На клієнтських комп'ютерах виконуємо додавання до домену (рис. 3.4). Після перезавантаження комп'ютера, можемо авторизуватись з логіном і паролем користувача.
5. На контролері домену відкриваємо консоль Управління груповою політикою.

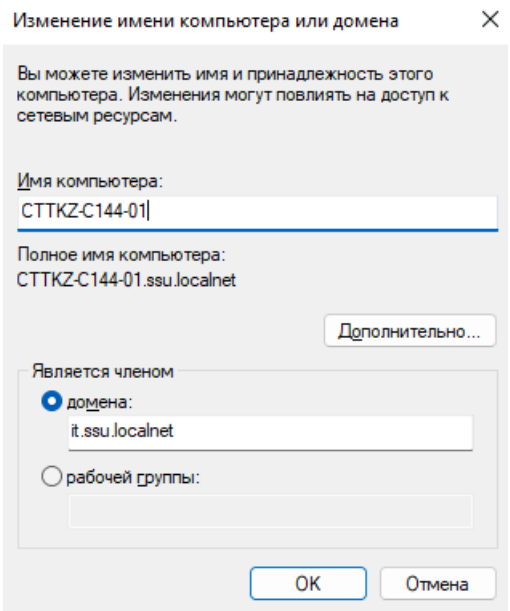

Рисунок 3.4 –Додавання до домену клієнтських комп'ютерів

6. У дереві it.ssu.localnet створюємо Новий об’єкт групової політики з назвою Drive Map Кафедра IT (рис. 3.5).

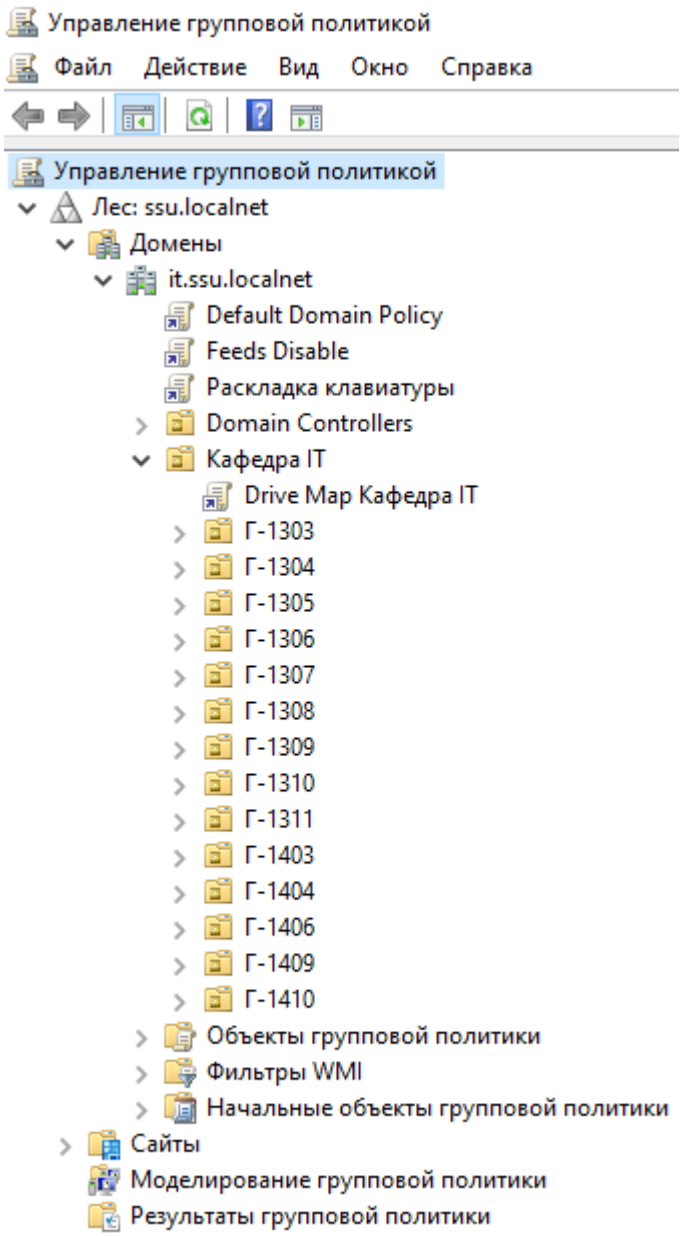

Рисунок 3.5 – Створення об’єктів групової політики

7. Змінюємо новостворену політику згідно наших задач з доступу до мережевих ресурсів (мережевих дисків) [17]. На прикладі (рис.3.6) (рис.3.7) вказано шляхи до фізичного мережевого сховища інформації.

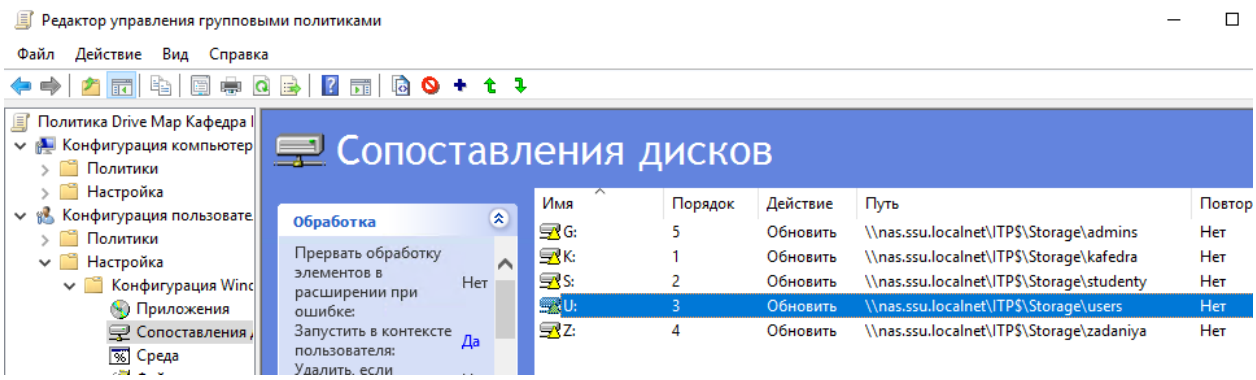

Рисунок 3.6 – Зміна політик доступу до мережевих ресурсів

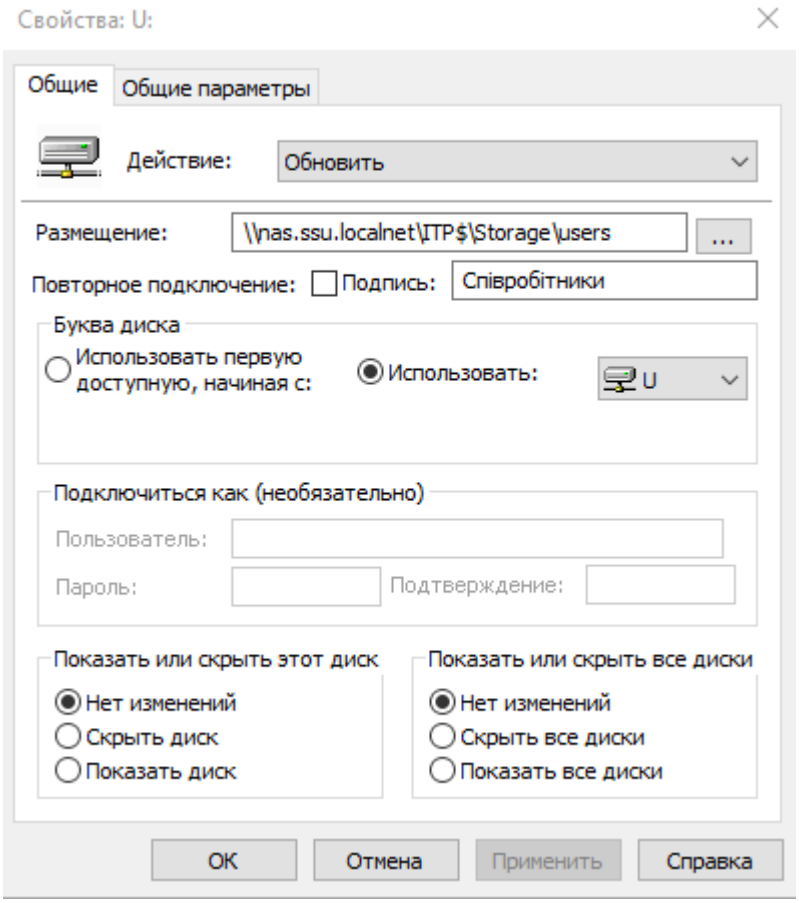

Рисунок 3.7 – Додавання шляхів до фізичного мережевого сховища

8. Обов’язково на вкладинці Загальні параметри зазначаємо націлювання групової політики на рівень елементу Група користувачів згідно раніше прийнятої політики доступу (рис. 3.8).

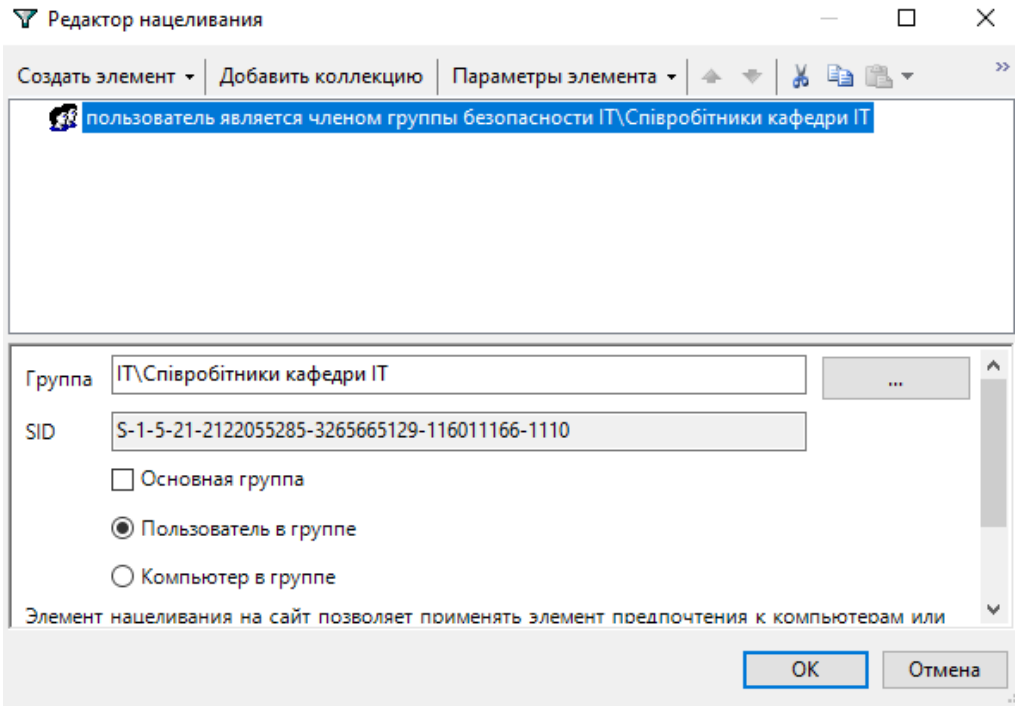

Рисунок 3.8 – Додавання шляхів до фізичного мережевого сховища

3.2.2 Мережеве сховище даних

Налаштування мережевого сховища даних (далі – МХД) для потреб кафедри IT включає в себе наступні кроки:

1. Згідно раніше прийнятої політики доступу, створюємо на МХД каталоги для зберігання інформації[18]. Назви каталогів краще писати латиницею (рис.3.9).

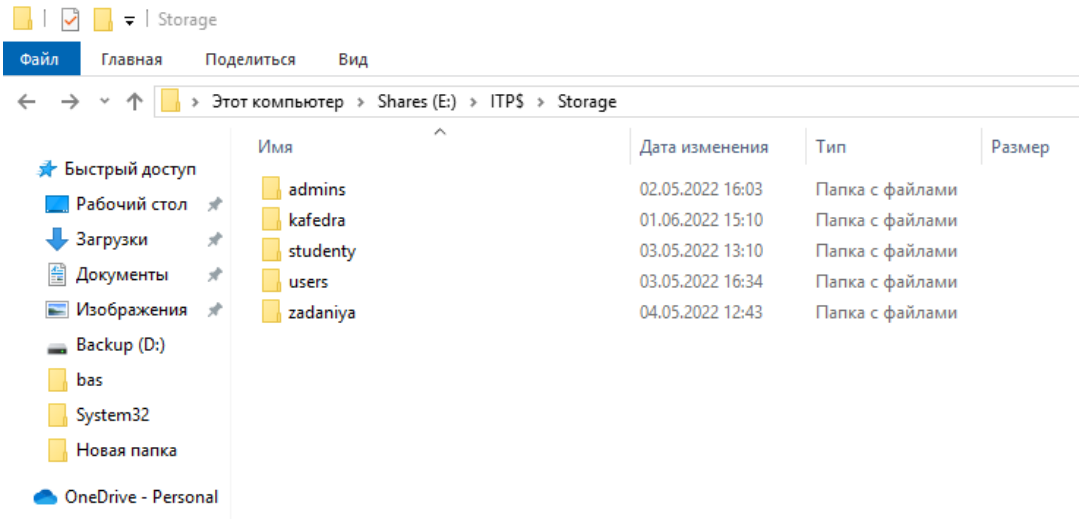

Рисунок 3.9 – Налаштування каталогів мережевого сховища даних

2. В параметрах загального доступу кожного каталогу дозволяємо доступ з мережі та, у вкладинці Безпека, додаємо групу користувачів, згідно нашої політики доступу (рис.3.10).

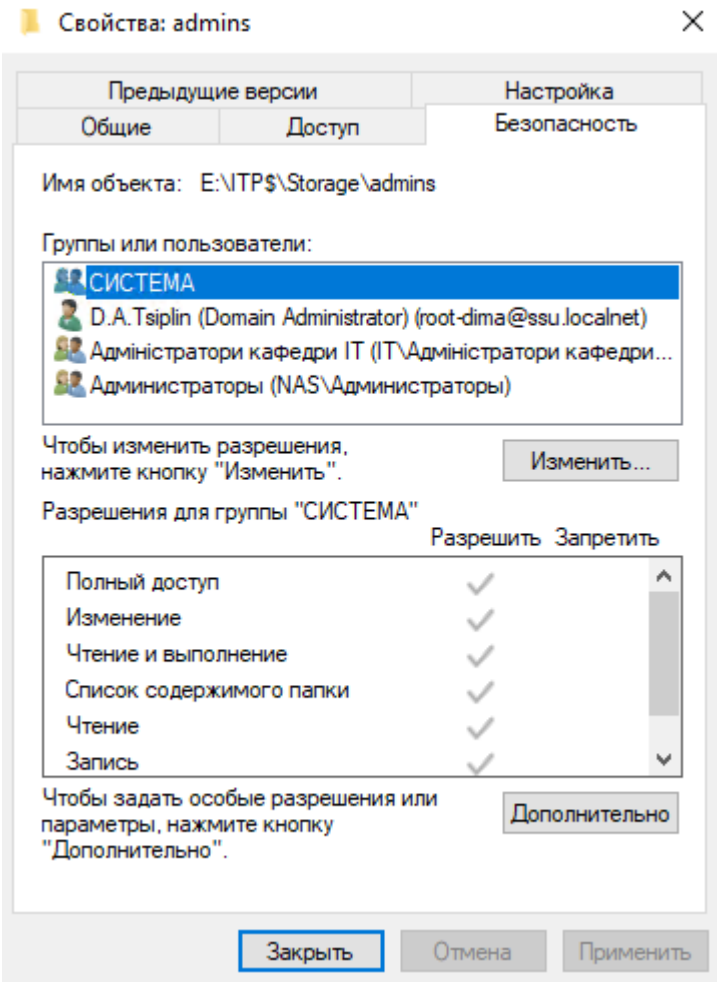

Рисунок 3.10 – Налаштування доступу до каталогів мережевого сховища даних

Таким чином виконано налаштування безпечного зберігання інформації на мережевому сховищі з автоматичним підключенням мережевих дисків до профілю користувачів. Під час логіну користувача, перевіряються права доступу до кожного з каталогів на сховищі, та підключаються дозволені мережеві диски.

3.2.3 Endpoint Configuration Manager

Налаштування системи Endpoint Configuration Manager (далі – ECM) проведено заздалегідь та використовується, як основна система віддаленого керування програмним забезпеченням СумДУ[19]. Для кафедри ІТ було створено еталонний образ операційної системи (рис.3.11).

Значок	Имя	Версия	Комментарий	Идентификатор образа	Версия ОС
	ITP-Windows-10-Pro.wim	21H1		SSU0002B	10.0.19041.928

Рисунок 3.11 – Образ еталонної операційної системи.

Також додано клієнти кафедри для керування програмним забезпеченням, операційними системами і засобами антивірусного захисту (рис.3.12). Додаткових налаштувань система ECM не потребує.

Имя	Клиент	Основные пользователи	Текущий пользователь...	Код сайта	Активность клиентов
G1303-01	Да			SSU	Активные
G1303-02	Да			SSU	Активные

Рисунок 3.12 – Додані клієнти кафедри ІТ.

3.2.4 Додаткові налаштування серверів

Сервери оновлення та активації операційних систем заздалегідь налагоджено для потреб СумДУ. Додаткові налагодження дані системи не потребують. Дії антивірусного захисту MS Endpoint Protection за замовченням встановлено згідно рисунка 3.13.

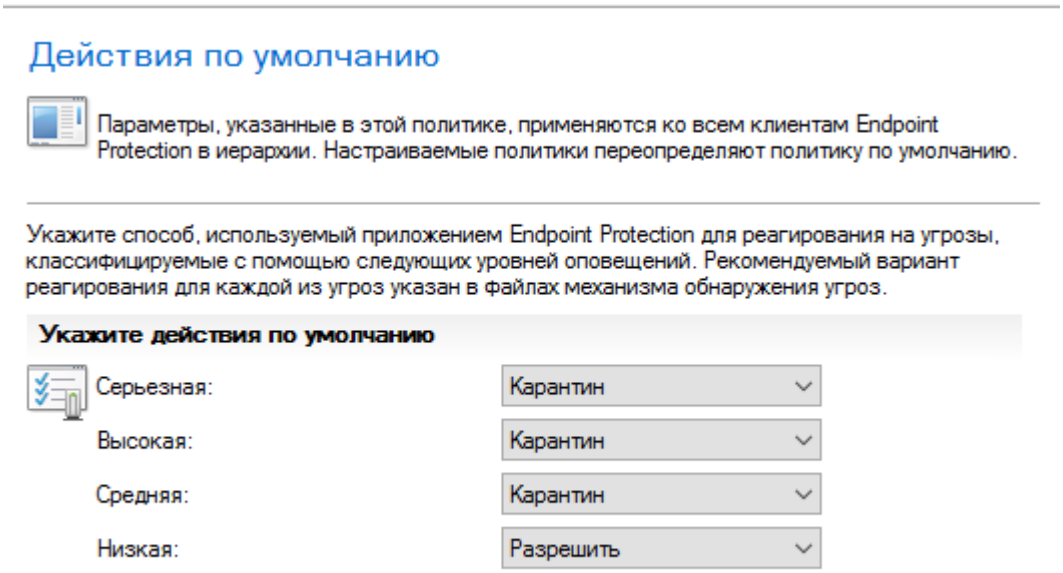

Рисунок 3.13 – Додані клієнти кафедри ІТ.

3.3 Тестування системи

Тестування працездатності системи зведене до перевірки доступу до загальних мережевих дисків згідно авторизації користувача (Табл.3.1). Також важливе своєчасне отримання оновлень програмного забезпечення та антивірусних сигнатур. Наявність локальної групової політики із вказанням серверу оновлення на клієнтській операційній системі дозволяє перевірити працездатність відпрацьованої групової політики, налаштованої на контролері домена (рис.3.14, 3.15). Перевірка авторизації користувача в домені **IT.SSU.LOCALNET** виконується за умови вдалого входу користувача до операційної системи клієнтського пристрою.

Таблиця 3.1 – Дозволи доступу користувачів кафедри IT.

Мережевий диск	Мережева папка на сховищі	Група користувачів
Адмін	E:\ITP$\Storage\admins	Адміністратори кафедри IT
Кафедра	E:\ITP$\Storage\kafedra	Співробітники кафедри IT
Студенти	E:\ITP$\Storage\studenty	Користувачі класів, Співробітники кафедри IT, Адміністратори кафедри IT
Співробітники	E:\ITP$\Storage\users	Співробітники кафедри IT
Завдання	E:\ITP$\Storage\zadaniya	Співробітники кафедри IT

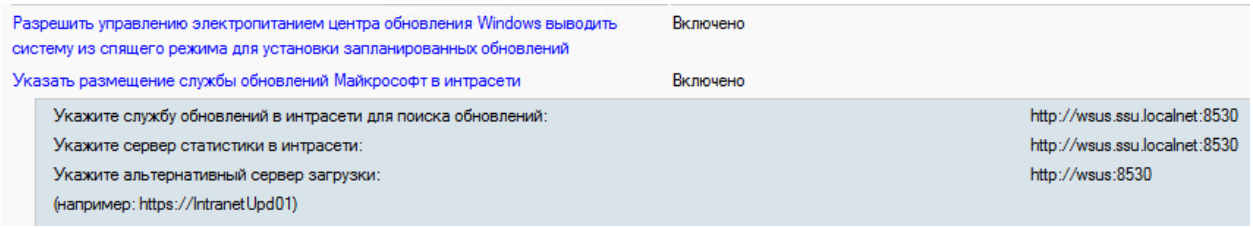

Рисунок 3.14 – Налаштування розташування серверу оновлень в мережі СумДУ.

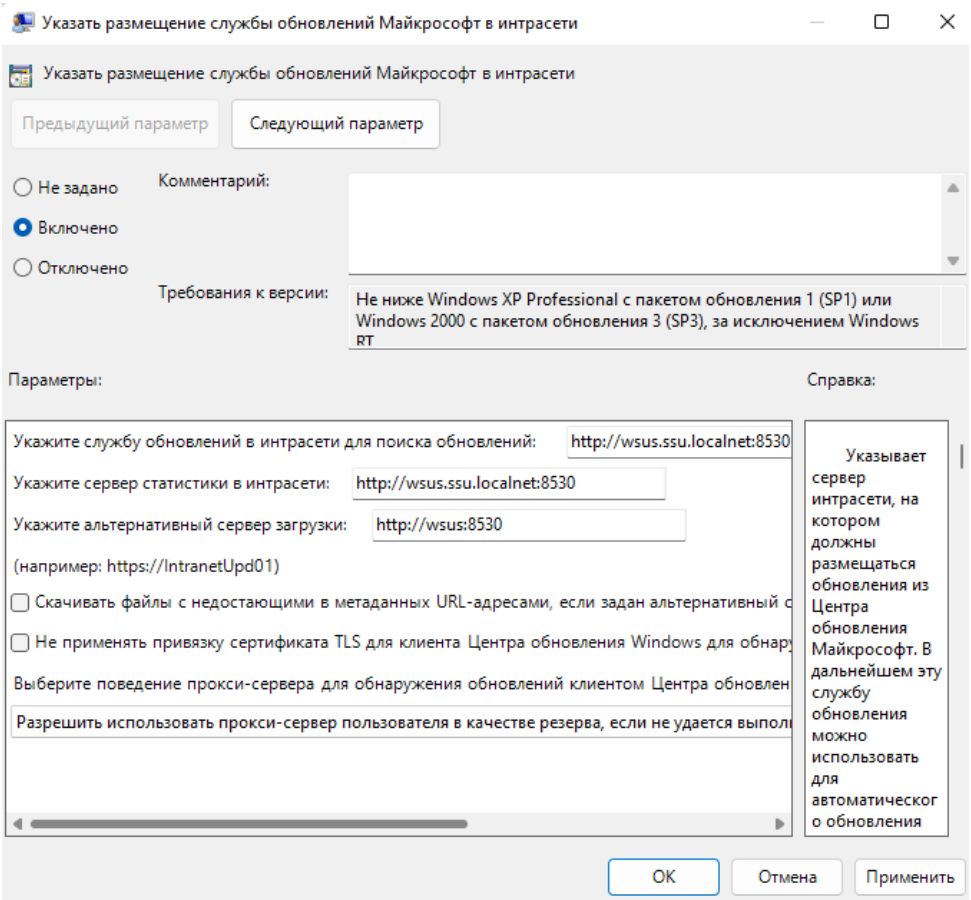

Рисунок 3.15 – Перевірка наявності локальної політики розташування серверу оновлення в мережу СумДУ

Таким чином, результати тестування доводять працездатність розробленої інформаційної системи з організації мережевого доступу кафедри ІТ СумДУ.

ВИСНОВКИ

В кваліфікаційній роботі було розв’язано практичну задачу розробки інформаційної системи з організації мережевого доступу випускової кафедри інформаційних технологій Сумського державного університету.

При цьому було виконано такі основні завдання:

1) Розміщено необхідні сервери, що підключені до загальної мережі СумДУ.

2) Виконано налаштування серверів згідно з потребами користувачів (співробітників, викладачів та студентів).

3) Створено та налаштовано мережеве програмно-апаратне сховище для збереження інформації.

4) Налаштовано систему забезпечення резервного копіювання інформації.

5) Перевірено працездатність інформаційної системи з організації мережевого доступу.

СПИСОК ЛІТЕРАТУРИ

1. Krause Jordan. Mastering Windows Group Policy: Control and secure your Active Directory environment with Group Policy Packt Publishing Ltd, 2018. — 408 p. — ISBN 978-1-78934-739-5
2. Francis Dishan. Mastering Active Directory: Design, deploy, and protect Active Directory Domain Services for Windows Server 2022 3rd Edition. — Packt, 2021. — 778 p. — ISBN 1801070393, 9781801070393.
3. Francis Dishan. Mastering Active Directory: Deploy and secure infrastructures with Active Directory, Windows Server 2016, and PowerShell 2nd Edition. — Packt Publishing, 2019. — 770 p. —ISBN 978-1-78980-020-3.
4. Dauti B. Windows Server 2016 Administration Fundamentals Packt Publishing Ltd.-2017.-390p.-ISBN-10 1788626567
5. Dauti Bekim. Windows Server 2016: How to setup your server (Desktop Experience) BekimDauti.com, 2016. — 181 p. — (From installation to setting up your server). — ASIN: B01NCJXA69.
6. David Michael. How to Install and Configure a Windows Server 2016 Domain Controller: A Step-by-step Guide for Installing and Setting Basic Security Settings for a Domain Controller Independently published, 2021. — 164 p. — ISBN B089GQM3QD.
7. Kranjac Sasha, Stefanovic Vladimir. Installation, Storage, and Compute with Windows Server 2016: Microsoft 70-740 MCSA Exam Guide: Implement and configure storage and compute functionalities in Windows Server 2016 Packt Publishing, 2019. — 325 p. — ISBN 978-1-78961-945-4.
8. Eckert Jason W. Hands-On Microsoft Windows Server 2019 3rd edition. — Cengage, 2021. — 914 p. — ISBN 978-0-357-43615-8.
9. Henderson Mark, Krause Jordan. Windows Server 2019 Cookbook: Over 100 recipes to effectively configure networks, manage security, and administer

workloads 2nd Edition. — Packt Publishing Ltd., 2020. — 650 p. — ISBN 978-1-83898-719-0.

10. Lee Thomas. Windows Server 2019 Automation with PowerShell Cookbook: Powerful ways to automate and manage Windows administrative tasks 3rd edition. — Packt Publishing, 2019. — 476 p. — ISBN 978-1789808537.
11. Henderson Mark, Krause Jordan. Windows Server 2019 Cookbook: Over 100 recipes to effectively configure networks, manage security, and administer workloads 2nd Edition. — Packt Publishing Ltd., 2020. — 650 p. — ISBN 978-1-83898-719-0.
12. Faridi Syed. Windows Server 2019 Administration: Lab Book Independently published, 2021. — 184 p. — ISBN 979-8731013017.
13. Amaris Chris. Microsoft System Center 2012 Unleashed SAMS, 2012. - 1032 p.
14. Asp A., Baumgarten A., Beaumont S., Buchanan S., Gasser D. Microsoft System Center 2016 Service Manager Cookbook Second Edition. — Packt Publishing, 2017. — 672 p. — ISBN 1786464896.
15. Bennett B., Daalmans P., Martinez S. Mastering System Center Configuration Manager – 2017 Методичні вказівки з успішного використання майстерності і досвіду спеціалістів для Configuration Manager 2012 R2 + Windows Intune, Copyright 2017 by John Wiley & Sons, Inc., Indianapolis, Indiana, SYBEX, рік видання 2017, стор. 1188
16. Henriksen N. Microsoft System Center 1511 Endpoint Protection Cookbook Second Edition. — Packt Publishing, 2017. — 217 p. — ISBN 978-1-78646-428-6
17. Bettany Andrew, Rhodes Chris. Windows Installation and Update Troubleshooting Apress, 2016. — 201 p. — ISBN 1484218264
18. Burgerhout Jeroen. Microsoft Exam MD-100 Windows 10 Certification Guide: Learn the skills required to become a Microsoft Certified Modern Desktop Administrator Associate Packt Publishing, 2020. — 442 p. — ISBN 978-1-83882-218-7.

19. Panek William. MCSA. Windows 10 Study Guide Sybex, 2016. — 578 p. — ISBN: 978-1119252306

ДОДАТОК

Створення нового користувача в домені **IT.SSU.LOCALNET**

```
New-ADUser -Name "User2" -GivenName "Test" -Surname "User2" -
SamAccountName "testuser2" -UserPrincipalName "testuser2@it.ssu.localnet" -
Path "OU= Кафедра IT,DC=it,DC=ssu,DC=localnet" -AccountPassword(Read-
Host -AsSecureString "Input Password") -Enabled $true
```

Масове створення користувачів в домені **IT.SSU.LOCALNET**

```
$domain=“@it.ssu.localnet”
Import-Module activedirectory
Import-Csv "C:\ps\new_ad_users.csv" | ForEach-Object {
$userSAM=$_.SamAccountName
        if (@(Get-ADUser -Filter "SamAccountName -eq
'$($_.SamAccountName)'").Count -ne 0) {
Add-Type -AssemblyName Microsoft.VisualBasic
$userSAM = [Microsoft.VisualBasic.Interaction]::InputBox("Користувач з
іменем $_.SamAccountName вже існує", 'Нове ім’я користувача?',
$_.SamAccountName)
}
$upn = $userSAM + $domain
$uname = $_.LastName + " " + $_.FirstName + " " + $_.Initials
$transLastName=Translit($_.LastName)
$transFirstName=Translit($_.FirstName)
$transInitials=Translit($_.Initials)
$transuname = $transLastName + " " + $transFirstName + " " + $transInitials
New-ADUser -Name $transuname `
-DisplayName $uname `
-GivenName $_.FirstName `
-Surname $_.LastName `
-Initials $_.Initials `
```

```
-OfficePhone $_.Phone `
-Department $_.Department `
-Title $_.JobTitle `
-UserPrincipalName $upn `
-SamAccountName $userSAM `
-Path $_.OU `
-AccountPassword (ConvertTo-SecureString $_.Password -AsPlainText -force) -
Enabled $true
}
```

Функція транслітерації:

```
function global:Translit {
param([string]$inString)
$Translit = @{
[char]'а' = "a"
[char]'А' = "A"
[char]'б' = "b"
[char]'Б' = "B"
[char]'в' = "v"
[char]'В' = "V"
[char]'г' = "g"
[char]'Г' = "G"
[char]'д' = "d"
[char]'Д' = "D"
[char]'Є' = "Є"
[char]'є' = "є"
[char]'ж' = "zh"
[char]'Ж' = "Zh"
[char]'з' = "z"
[char]'З' = "Z"
[char]'і' = "i"
```

```
[char]'І' = "I"
[char]'ї' = "j"
[char]'Ї' = "J"
[char]'к' = "k"
[char]'К' = "K"
[char]'л' = "l"
[char]'Л' = "L"
[char]'м' = "m"
[char]'М' = "M"
[char]'н' = "n"
[char]'Н' = "N"
[char]'о' = "o"
[char]'О' = "O"
[char]'п' = "p"
[char]'П' = "P"
[char]'р' = "r"
[char]'Р' = "R"
[char]'с' = "s"
[char]'С' = "S"
[char]'т' = "t"
[char]'Т' = "T"
[char]'у' = "u"
[char]'У' = "U"
[char]'ф' = "f"
[char]'Ф' = "F"
[char]'х' = "h"
[char]'Х' = "H"
[char]'ц' = "c"
[char]'Ц' = "C"
[char]'ч' = "ch"
```

```
[char]'Ч' = "Ch"
[char]'ш' = "sh"
[char]'Ш' = "Sh"
[char]'щ' = "shch"
[char]'Щ' = "Shch"
[char]'ь' = ""
[char]'Ь' = ""
[char]'е' = "e"
[char]'Е' = "E"
[char]'ю' = "yu"
[char]'Ю' = "Yu"
[char]'я' = "ya"
[char]'Я' = "Ya"
}
$outCHR=""
foreach ($CHR in $inCHR = $inString.ToCharArray())
{
if ($Translit[$CHR] -cne $Null )
{$outCHR += $Translit[$CHR]}
else
{$outCHR += $CHR}
}
Write-Output $outCHR
}
```