МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ І ПРИКЛАДНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КУЧЕР РУСЛАН ОЛЕГОВИЧ

Допускається до захисту:
В.о завідувача кафедри
інформаційних технологій
доктор. техн. наук, професор
_____ Наталія ВЕСЕЛОВСЬКА
«____»_____ 2026 р.

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ КОРИСТУВАЧАМИ ACTIVE DIRECTORY В КОРПОРАТИВНИХ СИСТЕМАХ

Спеціальність 122 Комп’ютерні науки

Кваліфікаційна (бакалаврська) робота

Керівник:
Олексій МОСКВІН, доцент кафедри
інформаційних технологій,
к. т. н.
_____

Оцінка: _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____

Вінниця – 2026

АНОТАЦІЯ

Дипломна робота присвячена розробці автоматизованої системи управління користувачами в корпоративному середовищі на базі служби каталогів Active Directory.

У роботі досліджено теоретичні основи функціонування корпоративних інформаційних систем та принципи управління обліковими записами користувачів. Проведено аналіз існуючих підходів до адміністрування користувачів у середовищі Active Directory, визначено їх недоліки, зокрема високу ймовірність помилок при ручному введенні даних та значні витрати часу.

У процесі виконання роботи було обґрунтовано доцільність автоматизації процесів створення та управління користувачами. Розроблено та реалізовано desktop-додаток, який забезпечує зручний графічний інтерфейс для введення даних користувача, вибору організаційних одиниць та груп доступу. Запропонована система дозволяє автоматизувати створення облікових записів, їх додавання до відповідних груп та розміщення у визначених структурних підрозділах.

Особливу увагу приділено реалізації механізмів інтеграції з Active Directory, перевірці коректності введених даних та забезпеченню безпеки доступу. Проведено тестування розробленого програмного забезпечення, яке підтвердило підвищення ефективності процесу адміністрування користувачів.

Практичне значення роботи полягає у можливості використання розробленого додатку в корпоративних інформаційних системах для спрощення роботи системних адміністраторів, зменшення кількості помилок та підвищення продуктивності.

Ключові слова: автоматизація, користувачі, обліковий запис, корпоративна система, Active Directory, OU, групи доступу, desktop-додаток.

ABSTRACT

This thesis is devoted to the development of an automated user management system in a corporate environment based on the Active Directory directory service.

The thesis examines the theoretical foundations of corporate information systems and the principles of user account management. An analysis of existing approaches to user administration in the Active Directory environment has been carried out, and their shortcomings have been identified, in particular the high probability of errors during manual data entry and significant time expenditure.

In the course of the work, the feasibility of automating user creation and management processes was substantiated. A desktop application has been developed and implemented, providing a user-friendly graphical interface for entering user data, selecting organisational units (OUs) and access groups. The proposed system enables the automation of account creation, their addition to relevant groups and placement within specified organisational units.

Particular attention was paid to implementing integration mechanisms with Active Directory, verifying the correctness of entered data, and ensuring access security. Testing of the developed software was carried out, confirming an increase in the efficiency of the user administration process.

The practical significance of the work lies in the possibility of using the developed application in corporate information systems to simplify the work of system administrators, reduce the number of errors and increase productivity.

Keywords: automation, users, account, corporate system, Active Directory, OU, access groups, desktop application.

ЗМІСТ

АНОТАЦІЯ 2
ВСТУП 5
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КОРИСТУВАЧАМИ В КОРПОРАТИВНИХ СИСТЕМАХ 7
1.1Поняття корпоративних інформаційних систем 7
1.2. Принципи управління обліковими записами та доступом 12
1.3. Архітектура та можливості служби каталогів Active Directory 16
РОЗДІЛ 2 АНАЛІЗ ТЕХНОЛОГІЙ ТА ПОСТАНОВКА ЗАДАЧІ РОЗРОБКИ . 22
2.1. Огляд інструментів адміністрування Active Directory (PowerShell, GUI-засоби) 22
2.2. Обґрунтування вибору технології розробки desktop-додатка 29
2.3. Постановка задачі розробки автоматизованої системи 34
РОЗДІЛ 3 ОПИС ФУНКЦІОНУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ADUserCreator 40
3.1. Опис функцій системи 40
3.2. Алгоритм створення користувачів 47
3.3. Візуальне відображення результатів розробки за допомогою UML 51
3.4. Перспективи розвитку системи 56
ВИСНОВКИ 60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 62

ВСТУП

Актуальність. Сучасна епоха стрімкого розвитку цифрових технологій та широкого впровадження корпоративних інформаційних систем актуалізує завдання побудови ефективного управління обліковими записами користувачів. Сьогодні велика кількість організацій надають перевагу службі каталогів Active Directory як універсальному інструменту централізованого керування доступом до внутрішніх інформаційних ресурсів. Проте, у реальних умовах процеси створення, модифікації та видалення облікових записів найчастіше виконуються вручну, що спричиняє значні часові витрати, підвищує ймовірність виникнення помилок і погіршує загальний рівень інформаційної безпеки. Незважаючи на наявні вбудовані інструменти управлі ння, автоматизація процесів адміністрування облікових записів, особливо з орієнтацією на зручну взаємодію через графічний інтерфейс, залишається недостатньо опрацьованою. Особливо актуальною залишається задача забезпечення спрощеного вибору організаційних одиниць і груп доступу в рамках процесу створення нових облікових записів. Тому постає нагальна потреба у розробці автоматизованої системи у формі desktop-додатку, що забезпечить зручне, швидке та безпечне управління обліковими записами користувачів в корпоративному середовищі.

Основною **метою** проведеного дослідження є розробка автоматизованої системи для управління користувачами в середовищі Active Directory у форматі desktop-додатку з підтримкою функціоналу вибору організаційних одиниць та груп доступу.

Для досягнення поставленої мети передбачено вирішення наступних завдань:

- Провести аналіз теоретичних основ управління обліковими записами в корпоративних інформаційних системах.

- Дослідити функціональні можливості та архітектурні особливості служби каталогів Active Directory.

- Ідентифікувати основні недоліки існуючих методів адміністрування користувачів.

- Узагальнити сучасні підходи до автоматизації управління обліковими записами.

- Розробити вимоги до програмної системи автоматизації.

- Сформувати архітектуру desktop-додатку для управління користувачами у середовищі Active Directory.

- Реалізувати функціонал створення нових користувачів із можливістю вибору організаційних одиниць і груп доступу.

- Виконати тестування і здійснити оцінку ефективності розробленого рішення у контексті різних сценаріїв використання.

Об’єктом даного дослідження визначено процес управління обліковими записами користувачів у межах корпоративних інформаційних систем.

Предметом дослідження виступають методи та інструментарій автоматизації процесів створення і управління обліковими записами користувачів у середовищі Active Directory.

Теоретична значущість роботи полягає у формалізації знань щодо методологій автоматизованого управління обліковими записами користувачів та вивченні потенціалу застосування служби каталогів у корпоративних інформаційних системах.

Практична значущість результатів дослідження полягає у створенні desktop-додатку, спроможного автоматизувати процеси управління користувачами, зокрема створення нових облікових записів, призначення прав доступу, а також зниження навантаження на адміністративний персонал підприємств.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ КОРИСТУВАЧАМИ В КОРПОРАТИВНИХ СИСТЕМАХ

1.1 Поняття корпоративних інформаційних систем

У сучасному світі розвиток інформаційних технологій відіграє важливу роль у підвищенні ефективності діяльності підприємств. Фактично, кожна організація, незалежно від її масштабу чи галузі, використовує інформаційні системи для обробки, зберігання та передачі даних. Особливу увагу серед таких технологій приділяють корпоративним інформаційним системам, які дозволяють інтегрувати всі бізнес-процеси підприємства в єдиний інформаційний простір. Корпоративна інформаційна система представляє собою комплекс засобів програмного забезпечення, технічного обладнання, баз даних, методів і процедур, що сприяють автоматизації управління підприємством. Вона допомагає ухвалювати рішення й координувати роботу всіх структурних підрозділів. Основною метою впровадження таких систем є оптимізація інформаційних потоків, скорочення витрат часу та ресурсів, а також забезпечення швидкого доступу до надійної та актуальної інформації, що, у свою чергу, сприяє покращенню ефективності організації [3].

Функціонал корпоративних інформаційних систем охоплює різноманітні аспекти діяльності підприємства: фінансовий менеджмент, виробництво продукції, логістику, управління персоналом, маркетинг і багато інших напрямків. Вони створюють єдину інформаційну платформу, завдяки якій усі підрозділи організації працюють зі синхронізованими даними. Це зменшує ймовірність дублювання інформації і значно покращує якість управлінських рішень. Головною особливістю КІС є їх інтегрованість здатність об’єднувати всі компоненти в одну злагоджену систему. Завдяки цьому зміни, що відбуваються в одному підрозділі підприємства, автоматично відображаються в усіх

пов’язаних частинах системи [1]. Такий принцип роботи гарантує цілісність даних і значно знижує ризик появи помилок.

Ще однією важливою характеристикою корпоративних інформаційних систем є їхня масштабованість можливість адаптуватися до зростання підприємства, збільшення обсягів інформації та кількості користувачів. Це особливо важливо для великих організацій, де чисельність облікових записів може сягати кількох тисяч або навіть десятків тисяч. Корпоративні інформаційні системи вирізняються високим рівнем надійності та захисту, що зумовлено їхньою ключовою роллю у забезпеченні обробки конфіденційної інформації, життєво важливої для функціонування підприємства. Одним із головних завдань таких систем є гарантування безпеки даних, зокрема їх захист від несанкціонованого доступу, втрати чи пошкодження. Центральним елементом у цьому контексті виступають системи управління доступом, які регулюють права користувачів щодо виконання певних операцій у межах інформаційної системи[4].

Основними функціями корпоративних інформаційних систем є:

- збір та обробка інформації;
- централізоване зберігання даних у базах;
- підтримка прийняття управлінських рішень;
- автоматизація бізнес-процесів;
- оптимізація комунікацій між функціональними підрозділами;
- контроль і аналіз діяльності підприємства.

Управління користувачами є однією з ключових складових КІС, оскільки саме через них відбувається взаємодія з системою. Для кожного користувача створюється окремий обліковий запис, де вказуються права доступу до інформаційних ресурсів. В умовах великих організацій значна кількість користувачів ускладнює адміністрування, що вимагає запровадження спеціалізованих механізмів. У зв’язку з цим широко впроваджується використання служб каталогів, як-от Active Directory, вони сприяють централізованому управлінню обліковими записами, групами користувачів та

мережними ресурсами. Застосування таких підходів дозволяє впровадити ієрархічну структуру даних, відповідно до якої користувачі можуть бути згруповані в організаційні одиниці залежно від структурного поділу підприємства. Класифікація корпоративних інформаційних систем здійснюється за різними критеріями, зокрема, за функціональним призначенням виділяють такі категорії КІС:

- ERP-системи (Enterprise Resource Planning) - інтегровані рішення для планування ресурсів підприємства;

- CRM-системи - платформи для управління взаємовідносинами з клієнтами;

- SCM-системи - інструменти для оптимізації ланцюгів постачання;

- HRM-системи - засоби управління людськими ресурсами.

Крім того ці системи класифікують за рівнями управління на стратегічні, тактичні та операційні. Стратегічні системи орієнтовані на формування та підтримку довгострокових рішень, тактичні спрямовані на середньострокове планування та контроль, а операційні системи забезпечують функціонування повсякденних процесів підприємства. Інформаційна безпека відіграє ключову роль у функціонуванні корпоративних інформаційних систем. У міру зростання кількості користувачів і обсягів даних зростає й ризик несанкціонованого доступу до конфіденційної інформації. Тому для забезпечення належного захисту важливо впроваджувати механізми автентифікації, авторизації та моніторингу дій користувачів, у цьому аспекті системи управління користувачами стають необхідною складовою будь-якої інформаційної корпоративної системи [4].

Сучасний розвиток корпоративних інформаційних систем повністю відповідає викликам часу і включає активне використання хмарних технологій, мобільних додатків, інструментів автоматизації та штучного інтелекту. Це створює можливості для підвищення гнучкості систем, забезпечення зручного доступу до даних незалежно від місця перебування, а також оптимізує бізнес-

процеси, роблячи їх ефективнішими. Попри переваги, впровадження та експлуатація систем супроводжуються низкою викликів.

Серед основних проблем можна виділити високі витрати на розробку та інтеграцію, складність налаштування систем для роботи зі вже існуючими платформами, необхідність навчання співробітників, а також потенційні ризики пов'язані із забезпеченням безпеки даних. Корпоративні інформаційні системи становлять ключовий інструмент для забезпечення ефективного управління сучасними підприємствами, оскільки вони надають можливість комплексної автоматизації основних бізнес-процесів. Завдяки створенню інтегрованої інформаційної платформи, яка поєднує різні підрозділи організації, ці системи сприяють суттєвому підвищенню координації дій між відділами, скороченню дублювання операцій та зниженню частоти помилок у процесі обробки даних.

Серед ключових переваг корпоративних інформаційних систем слід зазначити зростання продуктивності праці співробітників, яке досягається завдяки автоматизації рутинних завдань, прискоренню обробки інформації та вдосконаленню документообігу. Це у свою чергу, сприяє більш раціональному використанню ресурсів підприємства, а також дозволяє працівникам зосереджувати зусилля на виконанні аналітичних та стратегічних завдань. Не менш важливим аспектом функціонування таких систем є організація управління користувачами. Правильний розподіл прав доступу та чітке регулювання ролей користувачів безпосередньо впливають на рівень захисту інформації й стабільність роботи системи в цілому. У зв'язку з цим зростає актуальність розроблення та впровадження інноваційних механізмів автоматизованого управління користувачами. Такі механізми дозволяють спростити процес адміністрування, посилити інформаційну безпеку та забезпечити доступ до даних відповідно до посадових обов'язків працівників, що створює підґрунтя для сталого розвитку підприємства[5].

Отже, корпоративна інформаційна система потребує не лише засобів зберігання даних про користувачів, а й інструментів їх стандартизованої обробки. Саме на цьому рівні виникає необхідність розробки прикладного

програмного забезпечення, яке поєднує зручний інтерфейс адміністратора з можливостями автоматичного виконання типових операцій у доменному середовищі.

У таких умовах ручне адміністрування поступово втрачає ефективність. Воно може бути прийнятним для невеликої кількості користувачів, однак під час масового створення облікових записів зростає ймовірність помилок, пов’язаних із людським фактором. До таких помилок належать неправильне написання логіна, вибір не того OU, пропуск обов’язкового атрибута, додавання до зайвої групи або відсутність користувача в потрібній групі доступу.

У навчальному закладі корпоративна інформаційна система має додаткову специфіку, оскільки користувачами є не лише працівники, а й студенти, викладачі, методисти, адміністративний персонал та тимчасові користувачі. Кожна категорія має власні вимоги до прав доступу, терміну дії облікового запису, належності до груп і доступних сервісів. Це підвищує актуальність засобів, які дозволяють швидко та стандартизовано створювати велику кількість облікових записів.

Особливе значення для корпоративних систем має узгодженість даних про користувачів. Якщо ПІБ, логін, поштова адреса або належність до підрозділу вказані некоректно, це може призвести до помилок у маршрутизації повідомлень, неправильного застосування групових політик або видачі доступу не до тих ресурсів. Тому автоматизація створення користувачів повинна включати не тільки сам факт створення запису, а й контроль якості вхідних даних.

Наявність єдиного підходу до керування обліковими записами дає змогу зменшити кількість дублювання даних і уникнути ситуацій, коли один і той самий користувач має різні ідентифікатори в різних підсистемах. Для адміністратора це означає спрощення супроводу, а для організації - підвищення контрольованості доступу до ресурсів. Саме тому централізовані служби каталогів стали одним із ключових елементів сучасної корпоративної IT-інфраструктури.

У контексті корпоративних інформаційних систем важливо розглядати користувача не лише як окремий обліковий запис, а як цифрову ідентичність, пов’язану з певною посадою, підрозділом, набором повноважень і доступом до інформаційних ресурсів. У великих організаціях така ідентичність використовується одночасно в декількох сервісах: доменній інфраструктурі, файлових сховищах, поштових системах, внутрішніх вебпорталах, системах електронного документообігу та навчальних платформах.

1.2. Принципи управління обліковими записами та доступом

У рамках корпоративних інформаційних систем ефективне управління обліковими записами та доступом до ресурсів виступає фундаментальним компонентом забезпечення стабільного й безпечного функціонування підприємства. Кожен користувач системи оперує через персоналізований обліковий запис, який встановлює його рівень доступу до інформаційних ресурсів, а також визначає відповідні права і повноваження. Недоліки в організації цього процесу можуть створити значні ризики, зокрема витоки даних, несанкціонований доступ до ресурсів або загальне порушення функціонування системи. Сучасні концепції управління доступом спираються на комплекс принципів, які спрямовані на досягнення рівноваги між зручністю користування системою та її захищеністю. Зазначені принципи впроваджуються через спеціалізовані технологічні засоби, серед яких особливу роль відіграє служба каталогів Active Directory, що забезпечує централізоване адміністрування користувачів, груп і політик доступу до корпоративних ресурсів.

Першою фазою взаємодії користувача з інформаційною системою є процес його ідентифікації та автентифікації. Ідентифікація полягає у встановленні особи користувача через унікальний ідентифікатор, як-от логін, тоді як автентифікація представляє собою процедуру підтвердження достовірності особи шляхом введення аутентифікаційної інформації, зазвичай пароля. Інноваційні методи

доступу також включають застосування багатофакторної автентифікації (multi-factor authentication), яка забезпечує додатковий шар захисту. Вона передбачає використання різних засобів підтвердження, наприклад одноразових кодів або біометричних ідентифікаторів. Такий підхід є особливо важливим в умовах зростаючих загроз кібербезпеки[5].

Після успішного проходження автентифікаційного процесу інформаційна система визначає перелік дій та можливостей, доступних для конкретного користувача. Цей етап називається авторизацією і базується на заздалегідь установлених політиках доступу, які регулюють права і обмеження щодо використання ресурсів системи. У корпоративних інформаційних середовищах авторизація часто впроваджується через концепцію ролей або груп. Наприклад, користувачі, включені до певної групи, автоматично отримують набір прав, відповідний даній ролі. У системі Active Directory цей механізм реалізується на основі використання груп безпеки, що дає змогу оптимізувати процес управління доступом і забезпечити його гнучкість та ефективність.

Одним із ключових принципів інформаційної безпеки є принцип мінімальних привілеїв. Його сутність полягає у наданні користувачам лише тих прав доступу, які є безпосередньо необхідними для виконання їхніх службових завдань. Дотримання цього принципу дозволяє мінімізувати ризики випадкового або навмисного порушення безпеки системи. Наприклад, звичайний користувач не повинен мати адміністративних привілеїв, якщо ці права не потрібні для його роботи. Цей принцип полягає у чіткому визначенні та обмеженні прав доступу для різних категорій користувачів. У корпоративному середовищі це досягається шляхом впровадження ролей, груп та політик безпеки. Існує кілька моделей розмежування доступу:

-Дискреційна модель, де власник ресурсу сам визначає доступ до нього.

-Мандатна модель, де доступ регулюється жорсткими системними політиками.

-Рольова модель, де права призначаються залежно від ролей користувача.

Найпоширенішою в корпоративній практиці є рольова модель, яка забезпечує ефективне управління доступом великої кількості користувачів. Централізоване управління обліковими записами базується на використанні єдиного джерела для зберігання інформації про користувачів та їх права доступу. Такий підхід значно спрощує процес адміністрування та підвищує рівень контролю над системою. Прикладом реалізації цього принципу є служба Active Directory, яка забезпечує централізоване керування всіма обліковими записами та правами доступу в межах корпоративного домену[6].

У великих організаціях стрімке зростання кількості користувачів впливає на складність ручного адміністрування. Саме тому автоматизація процесів управління обліковими записами є ключовим принципом, який сприяє оптимізації роботи. Автоматизований підхід дає можливість:

- значно скоротити час, необхідний для створення користувачів;
- мінімізувати ризик виникнення помилок;
- забезпечити єдині стандарти налаштувань;
- підвищити продуктивність діяльності адміністраторів.

У цьому контексті доцільно використовувати спеціалізовані програмні рішення, такі як desktop-програми, що інтегруються з Active Directory.

Ефективний контроль за діями користувачів складає базис системи безпеки. Він включає ведення детальних журналів подій, у яких відображаються всі важливі дії від входу в систему до зміни налаштувань або доступу до корпоративних ресурсів. Принцип життєвого циклу облікового запису заснована на управлінні обліковими записами, та система охоплює повний цикл їх існування, включаючи створення, зміну та видалення, цей процес відомий як життєвий цикл облікового запису. Ключові етапи життєвого циклу: реєстрація нового користувача, надання прав доступу, коригування налаштувань облікового запису та тимчасова деактивація або остаточне видалення користувача.

Автоматизація цих процедур забезпечує актуальність даних та запобігає накопиченню неактивних чи застарілих облікових записів. Управління обліковими записами та доступом відіграє стратегічну роль у функціонуванні

корпоративних інформаційних систем. Дотримання таких основних принципів, як мінімізація привілеїв, централізоване адміністрування, автоматизація процесів та суворий контроль, гарантує високий рівень безпеки та ефективність використання ресурсів.

Таким чином, управління обліковими записами є комплексним процесом, який поєднує організаційні, технічні та безпекові аспекти. Розробка ADUserCreator спрямована на автоматизацію саме початкового та найбільш масового етапу цього процесу - створення користувачів і підготовку їх до роботи в доменному середовищі.

Під час створення великої кількості користувачів значну роль відіграє якість вхідного списку. Дані можуть надходити з Excel-файлів, кадрових систем, навчальних баз або інших джерел. Якщо такі дані не перевіряються автоматично, помилки переходять у доменну інфраструктуру й надалі ускладнюють супровід. Тому автоматизована система повинна виконувати перевірку обов’язкових полів, нормалізацію тексту та формування службових атрибутів за єдиними правилами.

Важливим елементом керування доступом є аудит. Журналювання дій адміністратора дозволяє зберігати інформацію про те, які операції були виконані, коли вони були виконані та яким був результат. Для масового створення користувачів це має особливе значення, оскільки адміністратор повинен мати можливість перевірити, які записи створено успішно, а які потребують повторної обробки.

Принцип мінімально необхідних привілеїв передбачає, що користувач повинен отримувати лише ті права, які необхідні для виконання його функцій. У середовищі Active Directory це найчастіше реалізується через групи безпеки. Відповідно, процес створення користувача має включати не тільки додавання облікового запису до каталогу, а й коректне призначення груп відповідно до ролі або підрозділу.

На етапі створення користувача особливо важливими є коректність ідентифікаторів і відповідність правилам іменування. Логін, UPN та електронна

адреса мають бути не лише унікальними, а й зрозумілими для адміністратора та користувача. Уніфіковані правила формування таких атрибутів спрощують пошук об’єктів, налаштування прав доступу та подальший супровід інфраструктури.

Життєвий цикл облікового запису користувача охоплює декілька етапів: створення, первинне налаштування, надання доступу, зміну атрибутів, тимчасове блокування, відновлення доступу та остаточне видалення або архівування. Кожен із цих етапів має бути контрольованим, оскільки обліковий запис є точкою входу до інформаційних ресурсів організації.

1.3. Архітектура та можливості служби каталогів Active Directory

Каталожні служби становлять фундаментальну складову сучасних корпоративних інформаційних систем, забезпечуючи централізоване управління, обробку та адміністрування даних, які стосуються користувачів, ресурсів і політик доступу. Серед найпоширеніших і технічно досконалих рішень у цій сфері виділяється Active Directory. Ця служба широко застосовується в корпоративному середовищі для ефективної організації управління мережею та інфраструктурою підприємств. Active Directory це ієрархічна служба каталогів, створена компанією Microsoft для централізованого управління обліковими записами користувачів, комп’ютерами, групами та іншими об’єктами в мережі. Вона інтегрована в операційні системи Windows Server і забезпечує адміністрування доступу до ресурсів у доменних мережах. Ключова роль Active Directory полягає в наданні єдиного механізму для автентифікації та авторизації користувачів, а також у впровадженні політик безпеки та управлінні мережевими ресурсами.

Архітектура системи спирається на ієрархічну модель, яка складається з кількох основних компонентів [10]:

1.Дерево представляє найвищий рівень ієрархії в Active Directory, об’єднуючи один або кілька доменів зі спільною схемою даних та глобальним каталогом. Він формує межі безпеки всієї системи.

2. Домен є основною одиницею адміністрування, це логічна структура, яка включає об'єкти, такі як користувачі, комп’ютери та групи, що мають спільну базу даних і політики безпеки.

3. Організаційні одиниці дозволяють структурувати об’єкти всередині домену відповідно до організаційної структури компанії (наприклад, за відділами чи підрозділами). Вони також спрощують делегування адміністративних прав на різні рівні.

4. Об’єкти формують основний будівельний блок Active Directory. До них належать користувачі, комп’ютери, принтери, групи тощо. Кожен об’єкт має унікальний набір атрибутів, таких як ім’я, пароль або права доступу.

Контролер домену це сервер із встановленою службою Active Directory, який виконує функції автентифікації, авторизації й управління об’єктами. У мережах підприємств зазвичай використовується кілька контролерів домену для забезпечення відмовостійкості та балансування навантаження. Архітектура Active Directory включає декілька ключових компонентів, що формують її функціональні можливості й ефективність:

-Active Directory Domain Services - базова служба, яка відповідає за зберігання, організацію та управління об’єктами каталогів;

-Global Catalog (глобальний каталог) забезпечує доступ до інформації про всі об'єкти в межах лісу і прискорює процеси пошуку даних;

-Schema (схема) задає метамодель даних, визначаючи типи об’єктів та їх атрибути, що зберігаються в системі;

-Group Policy (групові політики) інструмент централізованого адміністрування системних налаштувань і політик безпеки. [11]

Для гарантування безпечного доступу до ресурсів Active Directory застосовує сучасні протоколи автентифікації, серед яких:

-Kerberos є основний механізм автентифікації, що забезпечує високу ступінь безпеки завдяки використанню квиткової моделі;

-LDAP (Lightweight Directory Access Protocol) - протокол для доступу до ієрархічно структурованих даних каталогу;

-NTLM - резервний протокол автентифікації, що використовується у випадках, коли Kerberos недоступний. Такий набір механізмів сприяє надійній ідентифікації користувачів і забезпечує ефективний контроль доступу до інформаційних ресурсів.

Система Active Directory пропонує широкий спектр функцій для організації й підтримки корпоративної інфраструктури, зокрема:

-централізоване управління обліковими записами користувачів та комп'ютерними об'єктами;

- створення та адміністрування груп безпеки для оптимізації доступу до ресурсів;

- розподіл адміністративних повноважень між різними рівнями організації;

-реалізація групових політик для реалізації єдиних стандартів налаштувань;

- інтеграція з іншими програмними системами, сервісами та платформами;

-підтримка ієрархічної структури організації для впорядкування управління ресурсами;

- забезпечення високого рівня безпеки та детального контролю доступу[12].

Важливим аспектом Active Directory є спроможність до автоматизації процесів адміністрування за допомогою потужних інструментів, таких як PowerShell-скрипти, або за допомогою спеціалізованого програмного забезпечення, ця здатність значно підвищує ефективність операційного управління корпоративною інфраструктурою. Контролери домену постійно синхронізують дані між собою для підтримання актуальної інформації у всій системі, що забезпечує її надійність і безперервність у роботі.

Active Directory це спеціалізована база даних, яка служить для ефективного зберігання та управління даними. Вона оптимізована для виконання великої кількості операцій із читання та пошуку, а також меншої кількості змін і оновлень. Структура даних у Active Directory є ієрархічною, легко масштабованою та розширюваною. До типових даних, що можуть зберігатися в каталозі, належать черги друку принтерів, контактна інформація користувачів і параметри конфігурації мережі або комп'ютерів.

Основою бази даних Active Directory виступають об'єкти та їхні атрибути, а всі визначення цих об'єктів та атрибутів утримуються в її схемі, вона має три основні розділи: домен, схема та конфігурація. Розділ домену включає такі елементи, як користувачі, групи, контакти, комп'ютери, організаційні підрозділи та інші об'єкти. Завдяки масштабованості системи користувачі можуть додавати власні класи або атрибути відповідно до потреб. Розділ схеми містить правила і визначення класів та атрибутів, які можна використовувати в системі. Натомість конфігураційний розділ зберігає дані про налаштування служб, структурних частин і сайтів. На рисунку 1.1 представлено структуру розділу домену в Active Directory.

Контролер домену відповідає за перевірку ідентичності та авторизацію всіх користувачів і комп’ютерів у мережі типу Windows. Він також забезпечує призначення та виконання політик безпеки для комп’ютерів, а також установлення чи оновлення програмного забезпечення. Наприклад, під час входу користувача до комп’ютера, який є частиною домену Windows, система здійснює перевірку пароля і визначає тип користувача чи це системний адміністратор, чи звичайний користувач. У роботі контролера домену використовуються протоколи LDAP версій 2 і 3, Microsoft Kerberos, а також DNS. У сучасних корпоративних системах Active Directory виступає ключовою платформою для впровадження автоматизованих рішень з управління користувачами. Завдяки наявності API та інтеграційних інструментів, можна розробляти програмні засоби, які автоматично виконують такі завдання створення облікових записів,

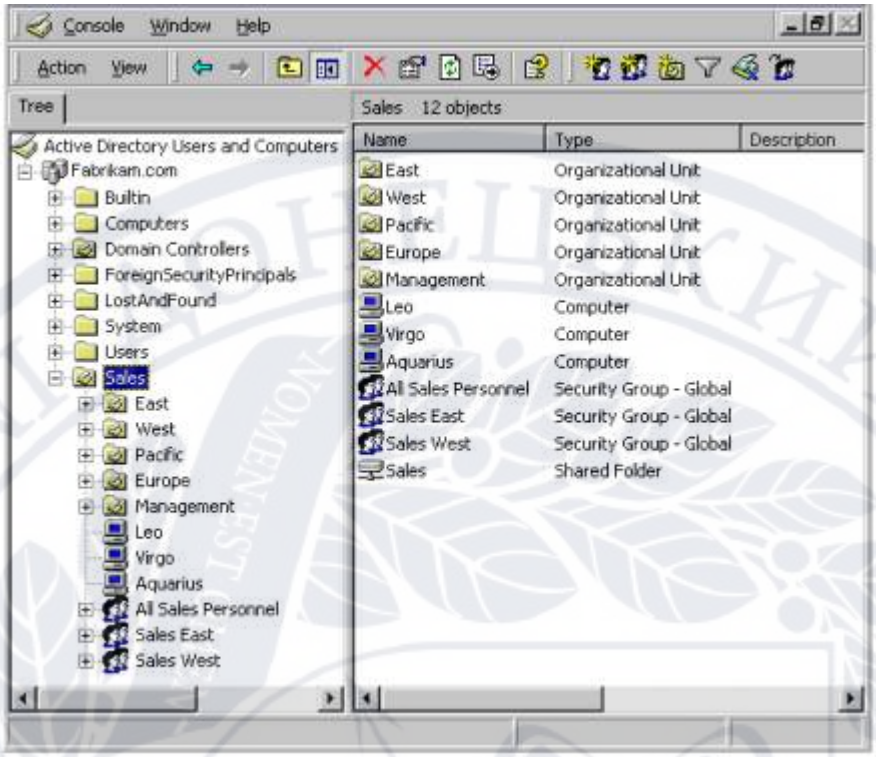

Рисунок 1.1 Приклад розділу "Домен" Active Directory

призначення прав доступу, додавання до груп, розміщення у організаційних одиницях. Це особливо актуально для розробки desktop-додатків, які надають адміністраторам зручний графічний інтерфейс для керування системами[2].

У корпоративному середовищі Active Directory забезпечує низку вагомих переваг:

- централізоване управління;
- підвищення рівня безпеки;
- скорочення адміністративних витрат;
- можливість масштабування;
- інтеграція з іншими продуктами Microsoft;
- підтримка автоматизованих процесів.

Попри численні переваги, система має і певні недоліки, зокрема складність налаштування та адміністрування; залежність від Windows-інфраструктури; необхідність у висококваліфікованих спеціалістах; потенційні ризики через

неправильну конфігурацію. Тому Active Directory є потужним інструментом для управління інформаційними системами компаній. Її архітектура гарантує гнучкість, масштабованість та високий рівень безпеки, що робить її базою для створення ефективних систем управління користувачами. Функціональність технології дозволяє створювати автоматизовані рішення, зокрема desktop-додатки, які значно полегшують адміністрування та сприяють підвищенню продуктивності підприємства.

РОЗДІЛ 2
АНАЛІЗ ТЕХНОЛОГІЙ ТА ПОСТАНОВКА ЗАДАЧІ РОЗРОБКИ

2.1. Огляд інструментів адміністрування Active Directory (PowerShell, GUI-засоби)

Отже, служба каталогів є не просто сховищем користувачів, а складною інфраструктурною платформою. Автоматизований інструмент створення користувачів повинен враховувати її ієрархію, механізми іменування, правила розміщення об’єктів, групову модель доступу та вимоги до контрольованості адміністративних дій.

У роботі Active Directory важливу роль відіграють DNS, LDAP/LDAPS і Kerberos. DNS забезпечує пошук контролерів домену, LDAP використовується для доступу до каталогу, а Kerberos відповідає за автентифікацію користувачів у доменному середовищі. Розуміння цих механізмів дозволяє правильно спроєктувати програму, яка взаємодіє з Active Directory через стандартні адміністративні засоби.

Групи Active Directory є основним механізмом надання доступу до ресурсів. Замість призначення прав кожному користувачу окремо адміністратор додає користувача до відповідних груп, а права призначаються вже на рівні цих груп. Це спрощує супровід і зменшує ризик помилок. Саме тому в ADUserCreator реалізовано вибір груп доступу як окремий етап перед створенням користувачів.

Організаційні одиниці OU використовуються для логічного групування об’єктів у межах домену. Вони дозволяють відображати структуру організації, застосовувати групові політики та делегувати адміністративні повноваження. Для автоматизованого створення користувачів вибір правильного OU є критично важливим, оскільки від нього можуть залежати політики безпеки, доступні ресурси та подальша схема адміністрування.

Користувацький об’єкт є одним із найважливіших елементів доменної інфраструктури. Він містить не лише ім’я користувача, а й логін, UPN, адресу електронної пошти, стан облікового запису, належність до груп і додаткові атрибути. Помилка в будь-якому з цих параметрів може вплинути на можливість входу користувача в систему або на доступ до корпоративних ресурсів.

Active Directory має об’єктну модель, у якій користувачі, групи, комп’ютери, організаційні одиниці та інші елементи подані як записи каталогу з набором атрибутів. Кожен об’єкт має унікальне розташування в ієрархії, що визначається distinguishedName, а також набір службових полів, які використовуються для автентифікації, авторизації, пошуку та застосування політик.

У сучасних корпоративних інформаційних системах управління користувачами, групами та ресурсами є однією з ключових функцій, яка прямо впливає на ефективність, безпеку і стабільність усієї організації. Будь-яке підприємство, яке використовує комп’ютерну інфраструктуру, стикається з необхідністю адміністрування великої кількості облікових записів, визначення доступу до інформаційних ресурсів і контролю дій користувачів у системі. У цих умовах дедалі актуальнішими стають централізовані підходи до адміністрування, що допомагають зменшити навантаження на системних адміністраторів і мінімізувати кількість помилок, спричинених людським фактором. Серед ключових компонентів подібних корпоративних систем виділяється служба каталогів Active Directory, яка забезпечує централізоване зберігання даних про всі об’єкти мережі. До її складу входять користувачі, комп’ютери, групи безпеки, принтери та інші ресурси. Завдяки ієрархічній структурі система дозволяє організовувати об’єкти у вигляді доменів і організаційних одиниць, які відображають реальну структуру підприємства. Це сприяє полегшенню процесу адміністрування та впорядкованості інформації в межах організації[1].

Однією з найбільших переваг Active Directory є можливість забезпечити централізоване управління всіма користувачами й ресурсами в одному місці. Це

дає адміністраторам змогу створювати, змінювати або видаляти облікові записи, призначати права доступу та контролювати активність користувачів без додаткового налаштування кожного пристрою окремо, такий підхід суттєво пришвидшує виконання задач і скорочує витрати часу на їх реалізацію. Ще одним важливим аспектом корпоративних інформаційних систем є захист даних. Користувачі повинні мати доступ тільки до тих ресурсів, які відповідають їхнім робочим функціям. Active Directory забезпечує таку сегментацію доступу через механізми автентифікації та авторизації. З їхньою допомогою система не лише ідентифікує користувача, але й визначає його права щодо використання окремих ресурсів.

Поширеність Active Directory у корпоративних системах пояснюється тим, що ця служба не обмежується зберіганням облікових записів. Вона виконує роль єдиного центру ідентифікації користувачів, комп'ютерів, груп, службових записів і ресурсів. Завдяки цьому організація може централізовано керувати доступом, застосовувати політики безпеки, контролювати зміни та підтримувати єдині правила роботи для локальної, гібридної або хмарної інфраструктури.

Важливою перевагою AD є інтеграція з іншими системами автентифікації та авторизації. На практиці служба каталогів може використовуватися разом із SSO-рішеннями, RADIUS-серверами для мережевого доступу, VPN або Wi-Fi, а також із сучасними федеративними механізмами, такими як OAuth та SAML через відповідні шлюзи або постачальники ідентичності. Це робить Active Directory базовим компонентом не лише локальної мережі, а й ширшої екосистеми керування цифровою ідентичністю.

Для управління компонентами Active Directory застосовуються різноманітні інструменти, які діляться на дві основні категорії: графічні та командні. Обидва підходи мають свої особливості та переваги, що впливають на їхній вибір залежно від специфіки задач. Графічні інтерфейси пропонують зручність використання завдяки інтуїтивному дизайну, який спрощує виконання базових операцій без потреби у вивченні командного синтаксису. Вони ідеально

підходять для виконання одиничних задач, як-от створення нового користувача, зміна його атрибутів або додавання до певної групи. Однак під час роботи з великою кількістю об’єктів графічні засоби можуть бути менш продуктивними через більшу витрату часу та зростання ризику помилок. Командні засоби забезпечують можливості автоматизації та значно прискорюють масове виконання операцій за допомогою скриптів, що особливо актуально в масштабних організаціях із великим обсягом об’єктів. Водночас їхнє застосування потребує володіння спеціальними технічними навичками та знань у програмуванні, що може стати викликом для менш досвідчених адміністраторів[5].

Рисунок 2.1 – Порівняння графічних та командних засобів адміністрування Active Directory

У результаті аналізу технологій управління користувачами в корпоративних інформаційних системах було встановлено, що служба каталогів Active Directory є ключовим інструментом для централізованого адміністрування облікових записів, груп і ресурсів. Вона забезпечує необхідний рівень інтеграції, безпеки та масштабованості, що закріплює її позицію як стандартного рішення для сучасних корпоративних мереж. Дослідження засобів адміністрування, зокрема графічних та командних інтерфейсів, виявило їхні переваги та

обмеження. Графічні інструменти характеризуються легкістю у використанні та дружнім інтерфейсом для користувачів. Водночас вони демонструють недостатню ефективність у виконанні масових операцій. Натомість командні інтерфейси забезпечують значно вищу продуктивність і дозволяють автоматизувати багато процесів, однак вимагають від адміністратора спеціальних знань і професійної підготовки.

На основі проведеного аналізу різних підходів та інструментів адміністрування було виявлено, що кожен із них має свої унікальні переваги, але також і певні обмеження, які не дозволяють їх універсально використовувати для вирішення всього спектра завдань, пов'язаних із управлінням користувачами в корпоративних інформаційних системах. Одні рішення відзначаються зручністю завдяки наявності графічного інтерфейсу, однак вони часто виявляються недостатньо ефективними для масових операцій чи виконання складних адміністративних завдань. Інші інструменти, хоча й забезпечують потужну функціональність через командний рядок або скрипти, вимагають від адміністратора високого рівня технічних знань, а в повсякденній експлуатації можуть бути менш зручними.

У результаті аналізу було встановлено, що наразі відсутнє універсальне рішення, яке б поєднувало легкість використання, широкий функціонал та гнучкі можливості налаштувань для управління користувачами. Це підкреслює потребу в розробці спеціалізованого програмного забезпечення у вигляді настільного додатка, який об'єднає зручність графічного інтерфейсу та потужність командних інструментів у рамках єдиної системи[9].

Основою для створення такого додатка має стати розробка інтуїтивно зрозумілого інтерфейсу, що значно спростить щоденні адміністративні завдання. Серед них створення нових облікових записів, їх редагування та блокування, управління групами користувачів і налаштування прав доступу. Крім того, важливим елементом стане інтеграція з командними утилітами та API Active Directory, що відкриє нові можливості для автоматизації складних сценаріїв. Адміністрування користувачів пов'язане з обробкою критично важливих даних

підприємства, тому необхідно забезпечити впровадження передових механізмів автентифікації, чіткого розподілу ролей і ведення докладних журналів користувацьких дій[8]. Це дозволить гарантувати прозорість процесів та підвищити рівень захисту інформаційної інфраструктури.

Запровадження подібної системи в корпоративне середовище позитивно вплине не тільки на продуктивність IT-спеціалістів, але й на загальну якість функціонування інформаційної інфраструктури підприємства. У довгостроковій перспективі це дозволить підвищити рівень автоматизації управлінських процесів, оптимізувати витрати на підтримку системи та забезпечити більш стабільну й безпечну роботу корпоративних мереж.

Порівняння графічних і командних засобів показує, що жоден із підходів окремо не є оптимальним для поставленої задачі. Графічний інтерфейс забезпечує зручність, а PowerShell - гнучкість і масштабованість. ADUserCreator розробляється саме як проміжне рішення, яке об’єднує ці переваги та зменшує недоліки обох підходів.

Для задачі створення користувачів важливою є також можливість попередньої перевірки даних. Стандартні графічні інструменти часто не орієнтовані на масову перевірку Excel-списків, а ручне виконання такої перевірки займає багато часу. Спеціалізована система може автоматично виявляти порожні поля, дублікати, некоректні символи, конфлікти логінів і помилки форматування.

Саме тому практичним рішенням є поєднання можливостей PowerShell з графічним інтерфейсом. Такий підхід дозволяє приховати складність команд від користувача програми, але зберегти потужність автоматизації. Адміністратор працює з формами, списками, кнопками та зрозумілими параметрами, а програма перетворює ці дії на відповідні операції Active Directory.

Командні засоби та PowerShell, навпаки, добре підходять для автоматизації повторюваних операцій. Вони дозволяють виконувати створення, зміну, пошук і видалення об’єктів за допомогою командлетів, а також обробляти списки користувачів із зовнішніх файлів. Проте використання командного рядка

вимагає від адміністратора уважності та знання синтаксису, оскільки помилка в параметрах може вплинути одразу на велику кількість об’єктів.

Під час аналізу засобів адміністрування Active Directory доцільно враховувати не тільки функціональність окремого інструмента, а й умови його практичного використання. Графічні засоби, такі як стандартні консолі адміністрування Windows Server, зручні для одиничних операцій і візуального перегляду структури домену, однак вони не забезпечують достатньої швидкості під час масової обробки користувачів.

Разом з тим обраний підхід не виключає подальшого розвитку системи. Логіка імпорту, генерації ідентифікаторів, створення користувачів і журналювання може бути використана як основа для майбутнього вебінтерфейсу або сервісного модуля. Таким чином, реалізація у вигляді desktop-додатка є доцільною для поточного етапу, але не обмежує можливості розвитку архітектури.

Ще одним аргументом на користь desktop-рішення є контрольованість середовища виконання. На відміну від вебзастосунку, який потребує серверної частини, налаштування вебсервера, автентифікації та захисту мережевих запитів, desktop-додаток може працювати безпосередньо на робочому місці адміністратора. Це спрощує первинне впровадження та зменшує кількість інфраструктурних залежностей.

Під час вибору технології також враховувалася можливість супроводу розробленого рішення в майбутньому. PowerShell є зрозумілим для системних адміністраторів, оскільки часто використовується в щоденній роботі з Windows Server. Це означає, що за потреби адміністратор може не лише користуватися готовою програмою, а й адаптувати окремі сценарії під внутрішні правила організації.

2.2. Обґрунтування вибору технології розробки desktop-додатка

Розробка автоматизованої системи управління користувачами в корпоративному середовищі є складним інженерним завданням, що передбачає вибір ефективного технологічного стеку, здатного забезпечити стабільну, безпечну й зручну роботу з обліковими записами. Головними критеріями для такого програмного забезпечення є інтеграція з корпоративною інфраструктурою, можливість централізованого управління користувачами, зручний адміністраторський інтерфейс та автоматизація рутинних завдань. У корпоративних інформаційних системах ключову роль відіграє служба каталогів Active Directory, яка слугує центральним сховищем даних про користувачів, групи, пристрої та інші мережеві ресурси. Саме через Active Directory реалізуються основні функції автентифікації, авторизації та доступу до ресурсів організації. Відповідно, система автоматизації управління користувачами повинна бути інтегрована з Active Directory, використовуючи її для всіх операцій над обліковими записами[10].

Одним із важливих завдань у цьому контексті є спрощення процесу створення та налаштування облікових записів користувачів. У великих організаціях, де кількість користувачів може досягати сотень чи навіть тисяч, ручне адміністрування стає неефективним через значні часові затрати і ймовірність людських помилок. Наприклад, неправильне налаштування груп доступу або вибір невідповідної організаційної одиниці можуть значно вплинути на функціонування системи. Таким чином, виникає потреба у створенні автоматизованого рішення, здатного забезпечити швидке та стандартизоване виконання задач із мінімальним втручанням адміністратора. Додатковою перевагою буде наявність інтуїтивно зрозумілого інтерфейсу, що зменшить необхідність використання складних команд чи скриптів. Оптимальним варіантом у цьому випадку вважається розробка desktop-додатка, цей підхід є найбільш відповідним для задач системного адміністрування у локальних або доменних середовищах. На відміну від веб-застосунків, desktop-платформи забезпечують тіснішу інтеграцію зі службами операційної системи та

корпоративної інфраструктури. Зокрема, вони дозволяють безпосередньо працювати з Windows API для управління Active Directory, мінімізуючи складність реалізації таких функцій, як створення, редагування чи видалення облікових записів.

Крім того, desktop-додатки демонструють високу продуктивність завдяки локальному виконанню операцій без залежності від стабільності інтернет-з'єднання. Ще однією ключовою перевагою є можливість створення багатофункціонального графічного інтерфейсу. Наочна візуалізація, наприклад, у вигляді дерева організаційних одиниць, списків груп безпеки чи інтерактивних форм введення даних, значно полегшує роботу адміністратора і сприяє зменшенню помилок при виконанні рутинних завдань. Таким чином, використання desktop-архітектури є виправданим рішенням, яке поєднує продуктивність, безпеку та зручність експлуатації. Це дозволяє розробити програмне забезпечення для ефективної роботи з Active Directory, автоматизації управлінських процесів і відповідності сучасним вимогам корпоративних інформаційних систем. Для вибору типу застосунку (Desktop-додаток) враховували переваги це високу продуктивність роботи без залежності від браузера; прямий доступ до системних API операційної системи; можливість глибокої інтеграції з Windows-інфраструктурою[12]. стабільність роботи в локальному середовищі; відсутність потреби у постійному інтернет-з'єднанні.

Desktop-додатки є традиційним і широко використовуваним підходом для створення адміністративних інструментів у корпоративних системах. Для задач управління користувачами в Active Directory саме desktop-архітектура є більш ефективною, ніж веб-рішення, оскільки забезпечує швидкий доступ до адміністративних функцій та мінімальну затримку при виконанні операцій. Для реалізації desktop-додатка найбільш доцільним є використання платформи «.NET», яка забезпечує тісну інтеграцію з Windows та службами каталогу. У рамках цієї платформи можуть використовуватись технології:

З урахуванням практичної реалізації проєкту ADUserCreator технологічний стек системи доцільно визначити як набір інструментів,

орієнтованих на адміністрування Windows-домену та автоматизацію Active Directory:

- PowerShell як основна мова реалізації адміністративної логіки;

- Windows Forms через .NET-класи для побудови графічного інтерфейсу desktop-додатка;

- ActiveDirectory PowerShell Module для створення користувачів, пошуку об’єктів[14], перевірки унікальності логінів і додавання до груп;

- модулі роботи з Excel для імпорту початкових списків користувачів;

- засоби формування PDF-документів та журналів виконання для передачі початкових облікових даних і контролю результатів.

Вибір PowerShell є обґрунтованим, оскільки ця технологія є стандартним інструментом адміністрування Windows Server та Active Directory. Вона забезпечує прямий доступ до командлетів керування доменом, дозволяє швидко автоматизувати повторювані операції, інтегрується з .NET-класами та може використовуватися як для сценаріїв командного рядка, так і для desktop-інтерфейсу. У межах цього проєкту PowerShell виступає не лише як мова сценаріїв, а як основа прикладної логіки системи.

Рисунок 2.2 – Етапи розробки автоматизованої системи управління користувачами

Використання PowerShell у поєднанні з .NET-класами забезпечує стабільну взаємодію з системними API операційної системи Windows, а також дає змогу скористатися наявними засобами для роботи з каталогами, графічним

інтерфейсом і файлами. Це спрощує процес розробки та підвищує надійність програмного продукту, оскільки більшість операцій адміністрування Active Directory виконуються через штатні командлети.

Реалізація графічного інтерфейсу за допомогою Windows Forms дозволяє створити зрозуміле та зручне середовище для адміністратора, забезпечуючи інтуїтивну взаємодію із системою. У рішенні передбачено вибір організаційних одиниць OU, груп безпеки, імпорт Excel-файлу, запуск процесу створення користувачів і перегляд результатів виконання.

Desktop-рішення також забезпечує високу продуктивність завдяки виконанню операцій локально або в межах корпоративної мережі без залежності від веб-браузера чи сторонніх сервісів. Такий підхід особливо ефективний для системного адміністрування, де важливими є швидкодія команд, контрольоване середовище виконання, доступ до доменних модулів і можливість роботи з локальними файлами.

Журналювання результатів роботи дозволяє перевірити виконання операцій після завершення масового створення користувачів. У журналі мають фіксуватися успішно створені записи, помилки, попередження, конфлікти ідентифікаторів і результати додавання до груп. Це підвищує прозорість роботи програми та дає адміністратору можливість швидко повернутися до проблемних записів.

Формування PDF-файлу з початковими обліковими даними є важливим з погляду організації процесу видачі доступу. Такий документ може бути використаний адміністратором для контрольованої передачі логіна, початкового пароля та супровідної інформації користувачу. Водночас система не повинна розкривати конфіденційні дані стороннім сервісам, тому генерація документа виконується локально.

Окрему роль у системі відіграє імпорт даних з Excel. У багатьох організаціях саме електронні таблиці залишаються найпоширенішим способом передавання списків користувачів між підрозділами. Тому підтримка Excel-

файлів дозволяє інтегрувати програму в уже наявний робочий процес без необхідності розгортання додаткової бази даних або складного серверного компонента.

Використання Windows Forms через .NET-класи забезпечує можливість побудови desktop-інтерфейсу без переходу до складнішої архітектури вебзастосунку. Для задачі адміністративного інструмента це є доцільним, оскільки програма орієнтована на запуск у контрольованому середовищі адміністратора, має взаємодіяти з локальними файлами та доменними модулями, а також виконувати операції в межах корпоративної мережі.

Вибір PowerShell як основи реалізації пояснюється тим, що ця технологія є природним інструментом адміністрування Windows-інфраструктури. Вона підтримує роботу з модулем ActiveDirectory, дозволяє використовувати командлети New-ADUser, Set-ADUser, Get-ADUser, Add-ADGroupMember та інші засоби, які безпосередньо призначені для керування об’єктами домену.

Важливою вимогою є передбачуваність результату. Після завершення роботи адміністратор повинен чітко розуміти, які користувачі були створені, які атрибути їм призначено, до яких груп вони додані та які записи не були оброблені через помилки. Саме тому журнал виконання є не допоміжною, а обов’язковою частиною системи.

Під час постановки задачі також необхідно враховувати, що автоматизація не повинна позбавляти адміністратора контролю. Навпаки, програма має виконувати рутинні операції, але ключові параметри - OU, групи доступу, джерело даних і запуск створення - повинні залишатися під контролем відповідальної особи. Це дозволяє поєднати швидкість автоматизації з адміністративною відповідальністю.

Окремим ризиком є дублювання облікових записів. У доменному середовищі створення двох користувачів з однаковими або дуже схожими ідентифікаторами може ускладнити адміністрування, пошук об’єктів і видачу доступу. Тому система повинна не тільки створювати новий запис, а й

попередньо перевіряти наявність користувача з таким самим SamAccountName, UPN або email. Така перевірка є важливою умовою надійності масової операції.

Практична потреба в автоматизації також пояснюється тим, що адміністратор часто працює з даними, які надходять з різних джерел і не завжди мають однакову структуру. Наприклад, у списках користувачів можуть відрізнятися порядок полів, наявність по батькові, написання прізвищ, використання апострофів, дефісів або літер українського алфавіту. Якщо такі особливості не врахувати, сформовані логіни можуть бути некоректними або незручними для подальшого використання.

2.3. Постановка задачі розробки автоматизованої системи

Постановка задачі розробки автоматизованої системи ґрунтується на потребі скоротити кількість ручних операцій під час створення користувачів у корпоративному домені. У великих організаціях адміністратор виконує багато однотипних дій: створює обліковий запис, визначає організаційну одиницю, заповнює атрибути, додає користувача до груп доступу, формує початковий пароль і фіксує результат виконання. Ручне виконання таких операцій збільшує витрати часу та підвищує ризик помилок.

Для коректної автоматизації цього процесу необхідно враховувати логічну структуру Active Directory. Служба каталогів організовує об’єкти у вигляді лісів, доменів та організаційних одиниць. На рисунку 2.3 показано загальну ієрархію лісу доменів, а на рисунку 2.4 - приклад організації об’єктів у підрозділи.

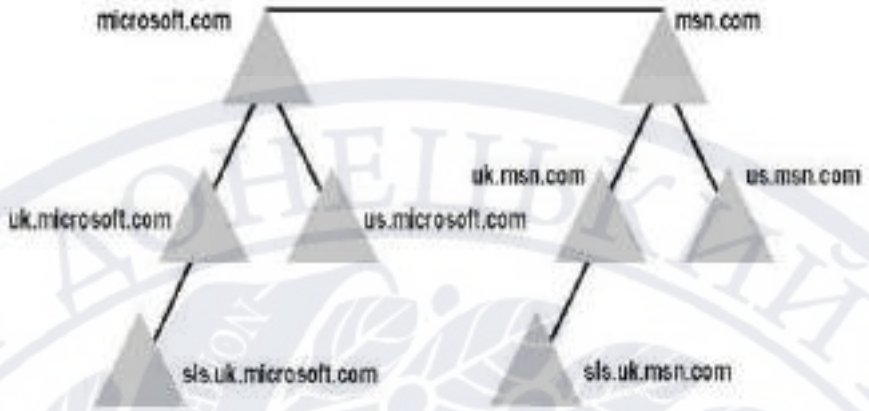

Рисунок 2.3 - Структура лісу доменів Active Directory

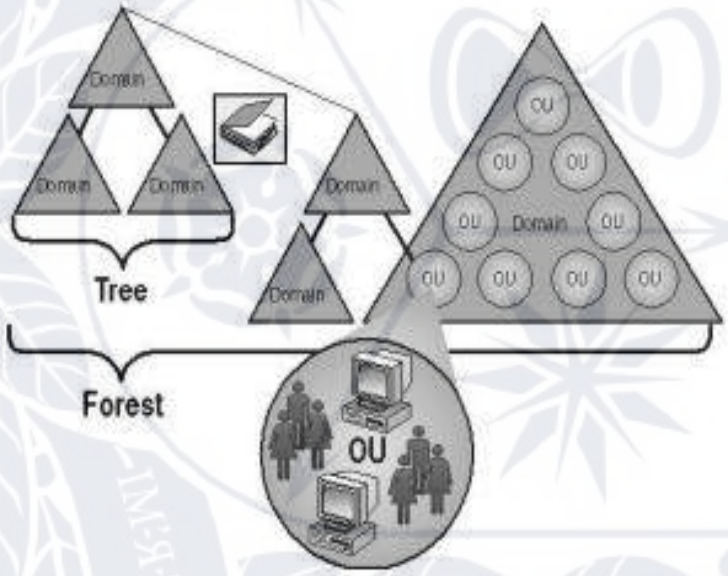

Рисунок 2.4 – Організація об’єктів у підрозділи

Фізична топологія Active Directory також має значення для стабільної роботи системи. Сайти, канали зв’язку та механізми реплікації впливають на швидкість пошуку об’єктів, застосування політик і час входу користувачів у систему. Приклад організації структури через сайти наведено на рисунку 2.5.

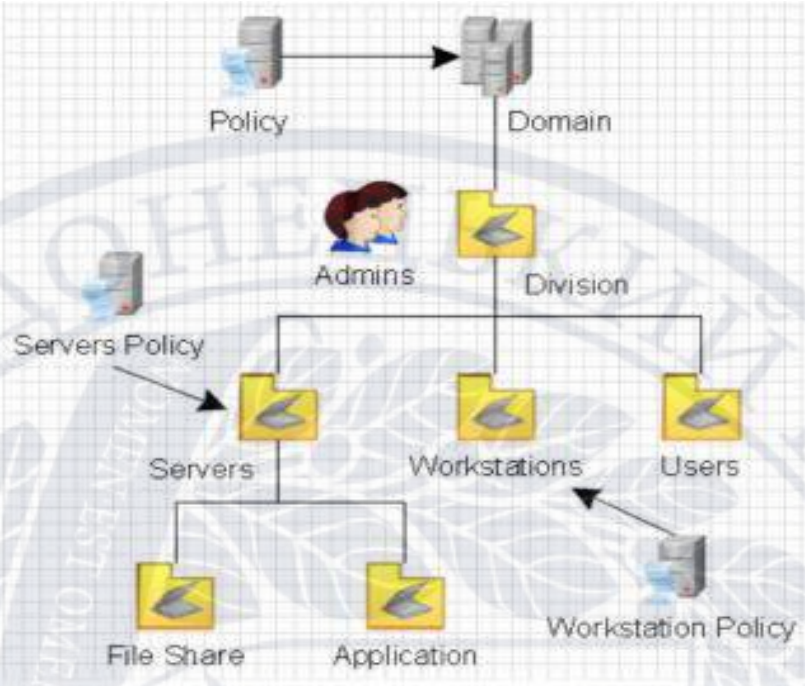

Рисунок 2.5 – Приклад організації структури через сайти

У контексті розробки ADUserCreator ключовими є не всі можливості Active Directory, а ті механізми, які безпосередньо використовуються під час створення користувачів. До них належать LDAP/LDAPS-запити або командлети Active Directory, класи об’єктів user, group, computer та organizational unit, атрибути SamAccountName, UserPrincipalName, email, а також списки контролю доступу й групові політики.

Доступ до даних каталогу через LDAP зображено на рисунку 2.6. Структуру каталогу простого домену Windows наведено на рисунку 2.7. Ці схеми демонструють, що обліковий запис користувача є лише одним із багатьох об’єктів, але саме він найчастіше створюється, змінюється і пов’язується з іншими елементами доменної інфраструктури.

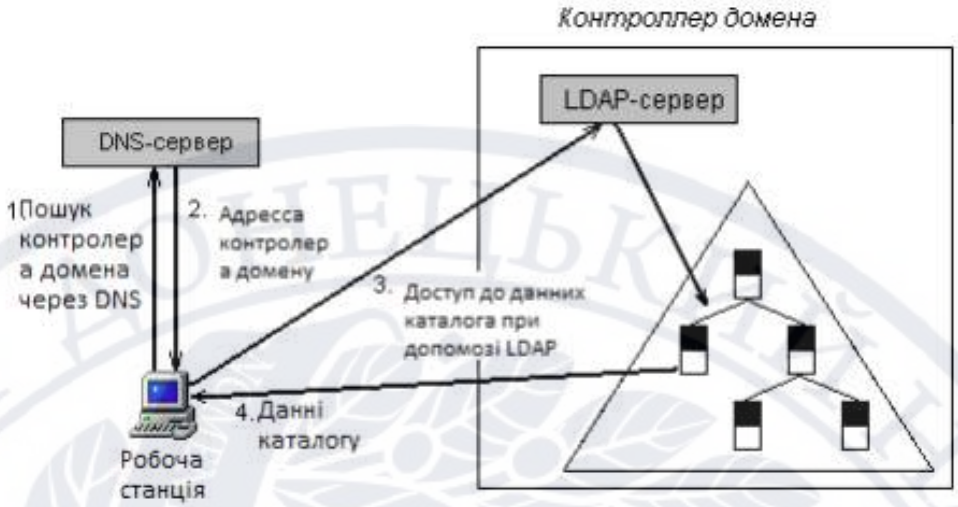

Рисунок 2.6 – Доступ до даних з використанням LDAP

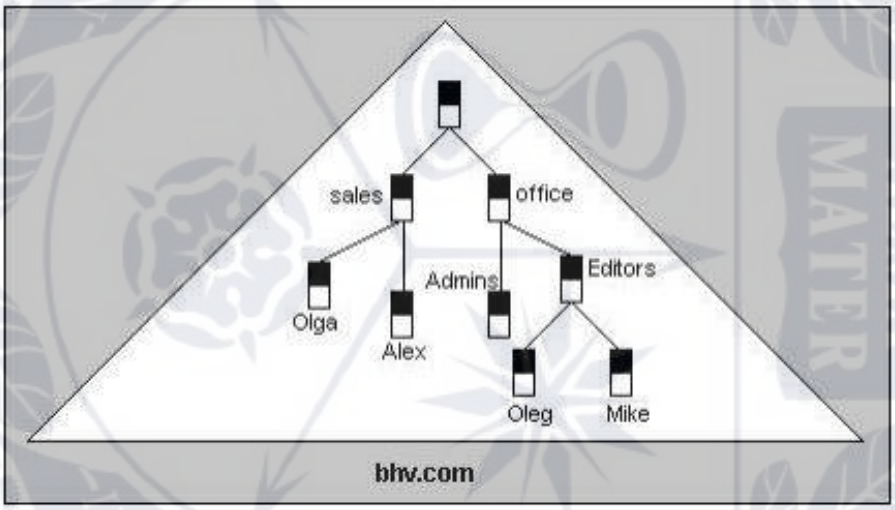

Рисунок 2.7 - Структура каталогу простого домену Windows

Отже, розроблювана система повинна автоматизувати прикладний сценарій роботи з об’єктами Active Directory, не замінюючи саму службу каталогів. Вона має використовувати наявну структуру домену, працювати з існуючими OU та групами, перевіряти унікальність облікових записів і фіксувати всі результати виконання.

Основні функціональні вимоги до системи ADUserCreator можна сформулювати так: імпорт даних користувачів з Excel-файлу; перевірка та нормалізація вхідних даних; транслітерація ПІБ; автоматичне формування SamAccountName, UPN та email; перевірка унікальності облікового запису; вибір

цільового OU; вибір груп доступу; створення користувача в Active Directory; генерація початкового пароля; формування PDF-файлу з обліковими даними; журналювання результатів виконання.

До нефункціональних вимог належать стабільність роботи в межах корпоративної мережі, сумісність з доменною інфраструктурою Windows, зрозумілий графічний інтерфейс, мінімізація ручних дій адміністратора, захист облікових даних і можливість подальшого аналізу журналу виконання.

Узагальнену роль Active Directory як центру керування ідентичністю та доступом показано на рисунку 2.8. Ця схема відображає зв'язок служби каталогів з LDAP/LDAPS, Kerberos, груповими політиками, DNS, аудитом та інтеграційними механізмами.

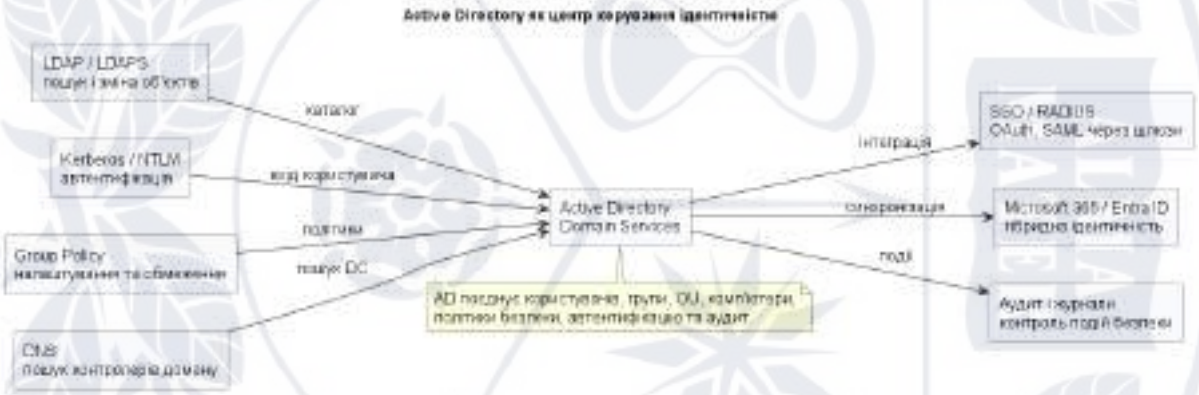

Рисунок 2.8 – Active Directory як центр керування ідентичністю та доступом

Сценарій обробки об'єктів у системі ADUserCreator наведено на рисунку 2.9. Він демонструє послідовність дій від завантаження Excel-файлу до створення користувача, додавання до груп, формування PDF-звіту та журналювання результату.

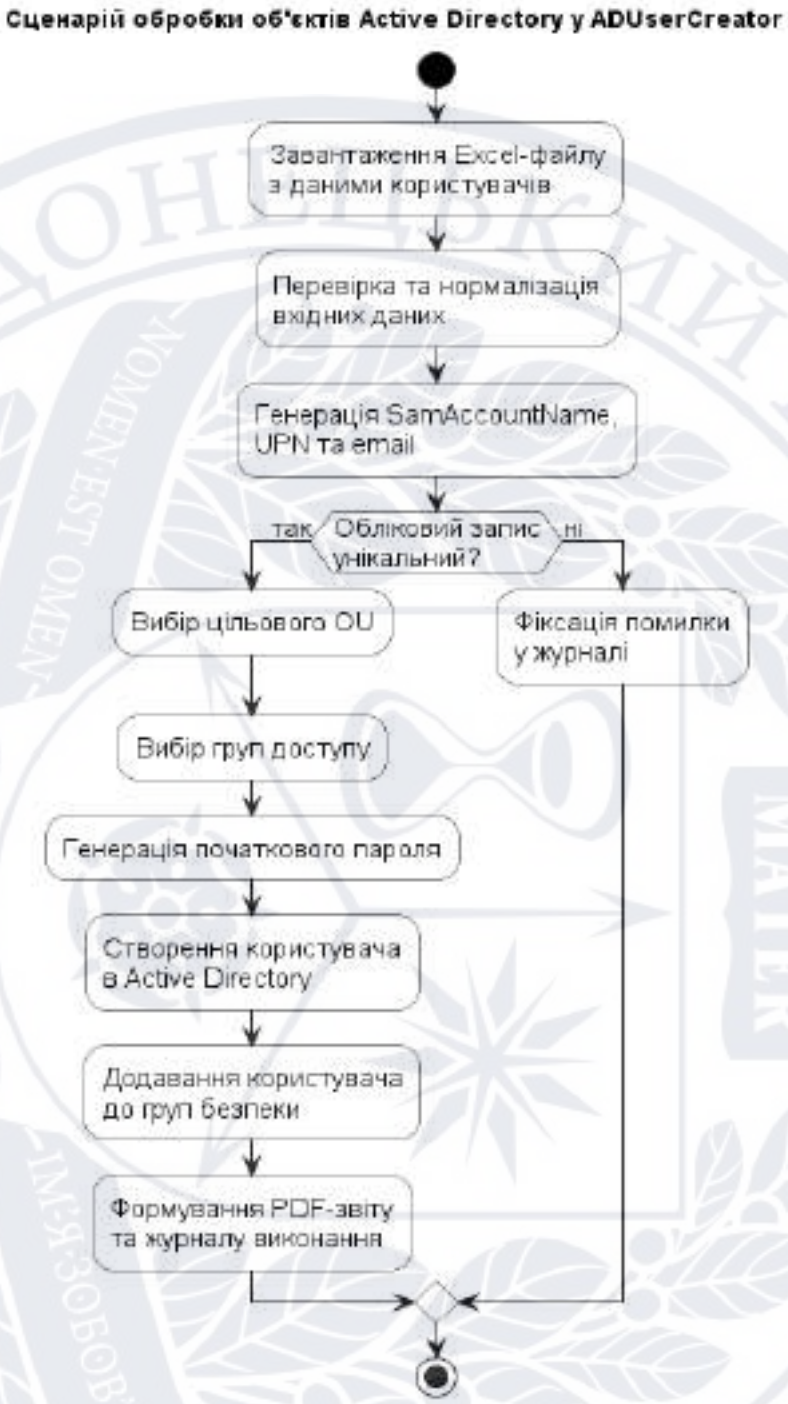

Рисунок 2.9 – Сценарій обробки об’єктів Active Directory у системі ADUserCreator

Таким чином, задача розробки полягає у створенні desktop-додатка, який формалізує типовий адміністративний процес створення користувачів Active Directory та об’єднує його в одному контрольованому інтерфейсі. Це забезпечує скорочення часу виконання операцій, зменшення кількості помилок і підвищення прозорості адміністрування доменної інфраструктури.

РОЗДІЛ 3
ОПИС ФУНКЦІОНУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ ADUserCreator

3.1. Опис функцій системи

Критеріями успішності розробки є скорочення часу створення користувачів, зменшення кількості ручних дій, зниження ризику помилок, можливість контролю результатів і зручність використання для адміністратора. Якщо система дозволяє швидко обробити список користувачів, сформувати коректні атрибути та зафіксувати результат, вона виконує свою основну прикладну функцію.

До обмежень системи належить залежність від наявності доменного середовища Windows і прав адміністратора або делегованих прав на створення користувачів у відповідних OU. Крім того, програма має працювати з урахуванням чинних політик паролів, правил іменування та обмежень, установлених у домені. Це означає, що ADUserCreator повинен адаптуватися до наявної інфраструктури, а не вимагати її перебудови.

Вихідними результатами роботи системи є створені облікові записи Active Directory, додавання користувачів до визначених груп, сформовані початкові паролі, PDF-файл з обліковими даними та журнал виконання. Наявність декількох видів результатів є важливою, оскільки адміністратор повинен не лише створити користувачів, а й мати підтвердження виконання операції.

Вхідними даними для системи є Excel-файл, який містить інформацію про користувачів. До таких даних можуть належати прізвище, ім’я, по батькові, підрозділ, група або інші службові поля, потрібні для формування облікового запису. Перед створенням користувачів система повинна перевірити, чи достатньо цих даних для виконання операції, та привести їх до єдиного формату.

Постановка задачі розробки ADUserCreator передбачає чітке визначення меж системи. Програма не замінює Active Directory, не змінює архітектуру домену та не виконує функції повноцінної системи керування ідентичністю. Її призначення полягає в автоматизації конкретного адміністративного сценарію - створення користувачів на основі підготовленого списку та застосування до них стандартних параметрів.

Система також має враховувати можливість повторного запуску або обробки частини списку. У практичній роботі адміністратор може отримати виправлений Excel-файл або потребу створити лише тих користувачів, які не були створені під час попередньої спроби. Наявність журналу та статусів виконання дозволяє швидше визначити, які записи потребують повторної уваги.

Функція формування атрибутів користувача має забезпечувати однаковість записів у домені. Якщо адміністратори створюють користувачів вручну, стиль написання логінів, email або службових атрибутів може відрізнятися. Автоматизоване формування за єдиним шаблоном дозволяє підтримувати порядок у каталозі та полегшує подальше адміністрування.

Однією з переваг ADUserCreator є те, що система може бути використана в типових сценаріях масового створення облікових записів: зарахування нових студентів, прийняття працівників, створення тимчасових користувачів, підготовка навчальних груп або формування доступу для окремих підрозділів. У кожному з цих випадків повторюються одні й ті самі дії, тому їх автоматизація дає помітний практичний ефект.

З погляду експлуатації система повинна бути зрозумілою для адміністратора без необхідності постійного звернення до вихідного коду або ручного виконання команд PowerShell. Інтерфейс має відображати основні параметри створення користувачів, дозволяти швидко обрати потрібні значення та запускати процес після перевірки даних. Такий підхід зменшує навантаження на адміністратора й підвищує повторюваність результату.

Розроблена система ADUserCreator призначена для автоматизації процесу створення облікових записів користувачів у середовищі Active Directory. Основним завданням системи є скорочення кількості ручних операцій адміністратора, уніфікація правил формування облікових даних, зменшення ймовірності помилок і прискорення масового створення користувачів у доменній інфраструктурі.

Система реалізована як desktop-додаток на базі PowerShell і орієнтована на роботу адміністратора домену. Вона поєднує імпорт вхідних даних з Excel, генерацію ідентифікаторів користувача, вибір організаційного підрозділу, призначення груп доступу, створення облікових записів, формування початкових паролів, підготовку PDF-файлу з обліковими даними та журналювання результатів виконання.

Рисунок 3.1 - Головне вікно desktop-додатку ADUserCreator.

Однією з ключових функцій системи є імпорт даних користувачів з Excel-файлу. Такий підхід дозволяє використовувати попередньо підготовлені списки

студентів, співробітників або інших категорій користувачів. Після завантаження файлу система виконує перевірку рядків, очищення зайвих пробілів, контроль наявності обов’язкових полів і підготовку даних до створення облікових записів.

Наступною важливою функцією є автоматичне формування ідентифікаторів користувача. На основі ПІБ система генерує SamAccountName, UserPrincipalName та адресу електронної пошти. Для цього застосовується нормалізація тексту і транслітерація, що забезпечує єдиний формат логінів та поштових адрес у межах доменної інфраструктури.

Перед створенням облікового запису система перевіряє унікальність сформованих значень. Перевіряється наявність користувача з таким самим SamAccountName, а також зайнятість електронної адреси або пов’язаних SMTP-адрес. У разі виявлення збігу система може змінити сформований логін відповідно до заданого правила або повідомити адміністратора про необхідність перевірки.

Для правильного розміщення користувачів у структурі домену передбачено вибір цільового організаційного підрозділу OU. Це дозволяє одразу створювати облікові записи в потрібному контейнері, де надалі можуть застосовуватися відповідні групові політики, правила доступу та адміністративні обмеження.

Окремим функціональним блоком є робота з групами Active Directory. Адміністратор може вибрати перелік груп, до яких мають бути додані нові користувачі. Після успішного створення облікового запису система автоматично виконує додавання користувача до зазначених груп, що зменшує кількість повторюваних дій і забезпечує однакові правила доступу для користувачів однієї категорії.

Для кожного нового облікового запису система генерує початковий пароль. Генерація виконується локально, без передавання паролів до зовнішніх сервісів. Після створення користувачів система формує PDF-файл з початковими обліковими даними, який може бути використаний адміністратором для передачі інформації користувачам у контрольований спосіб.

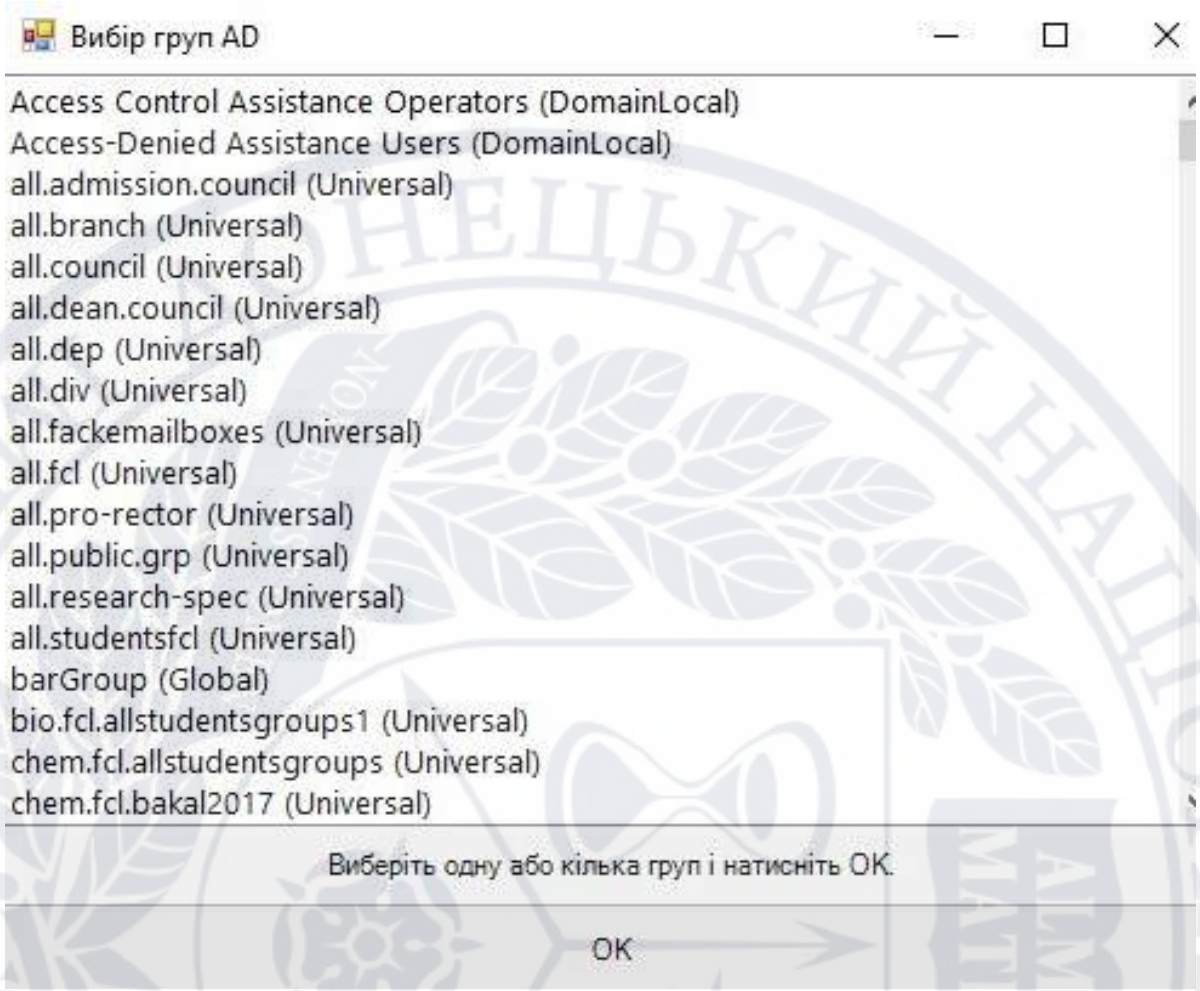

Рисунок 3.2 - Вибір організаційного підрозділу та груп доступу.

Система також веде журнал виконання операцій. У ньому фіксуються основні етапи роботи: початок обробки, результати перевірок, створення облікового запису, додавання до груп, виникнення помилок і попереджень. Журналювання дає змогу контролювати результат виконання, аналізувати причини помилок і підтверджувати факт виконання адміністративних дій.

Таким чином, ADUserCreator об’єднує в одному інструменті імпорт даних, автоматизоване формування атрибутів, створення користувачів, призначення груп доступу, генерацію початкових паролів, формування PDF-звіту та журналювання. Це робить систему практичним засобом автоматизації типових завдань адміністрування Active Directory.

Формування PDF-файлу та журналу виконання завершує робочий цикл системи. PDF-документ використовується для передачі початкових облікових даних, а журнал є інструментом контролю. Завдяки журналюванню

адміністратор може перевірити статус кожного користувача, побачити причини помилок і підтвердити факт виконання масової операції.

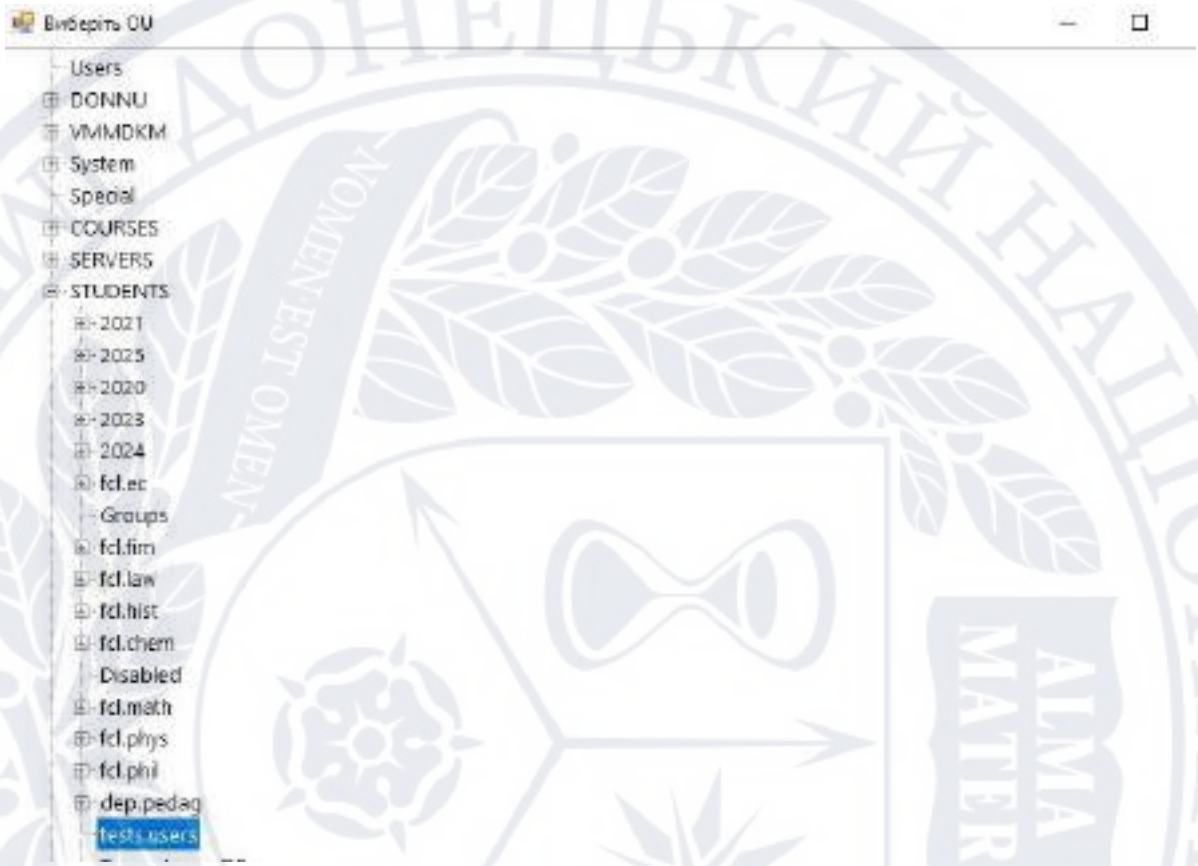

Рисунок 3.3 - Вибір груп в Active Directory.

Модуль вибору груп доступу дозволяє адміністратору заздалегідь визначити, до яких груп мають бути додані створені користувачі. Це спрощує видачу прав і зменшує кількість додаткових дій після створення облікового запису. У разі помилки додавання до групи система повинна зберегти відповідне повідомлення в журналі, щоб адміністратор міг виконати повторну перевірку.

Модуль вибору OU забезпечує розміщення користувачів у правильній частині структури Active Directory. Це важливо, оскільки від OU можуть залежати групові політики, правила делегування, сценарії входу та інші параметри середовища. Графічний вибір OU зменшує ризик помилкового введення distinguishedName вручну.

Генерація ідентифікаторів користувача виконується за єдиними правилами, що забезпечує стандартизацію облікових записів у домені. Система формує SamAccountName, UPN та email на основі ПІБ або інших вхідних даних. Якщо сформований ідентифікатор уже існує, програма повинна застосувати механізм уникнення дублювання або зафіксувати помилку для подальшого аналізу.

Функція імпорту даних є початковою точкою роботи системи. Вона забезпечує завантаження списку користувачів з Excel-файлу та перетворення рядків таблиці у внутрішні об’єкти програми. На цьому етапі важливо не лише прочитати файл, а й перевірити його структуру, визначити наявність обов’язкових колонок і підготувати дані до подальшої обробки.

Формування підсумкового PDF-документа має відбуватися після завершення основних операцій, коли вже відомо, які користувачі створені успішно. Це дозволяє уникнути потрапляння до документа даних про користувачів, для яких операція не завершилася. Водночас журнал має містити інформацію як про успішні, так і про невдалі записи, щоб адміністратор міг проаналізувати повну картину виконання.

Під час генерації пароля система повинна враховувати вимоги доменної політики. Якщо пароль не відповідає складності, довжині або іншим обмеженням, створення користувача може завершитися помилкою. Тому генерація початкового пароля має бути узгоджена з політиками безпеки організації та не повинна вимагати ручного виправлення після створення запису.

Ще одним важливим аспектом є послідовність виконання операцій. Спочатку мають виконуватися всі перевірки, потім формування ідентифікаторів, після цього створення користувача, і лише потім додавання до груп. Така послідовність дозволяє уникнути ситуацій, коли неповністю підготовлений або некоректний об’єкт потрапляє до доменної інфраструктури.

У процесі виконання алгоритму особливе значення має обробка помилок. Помилка в одному рядку Excel-файлу не повинна призводити до зупинки всієї операції, оскільки це зменшило б ефективність масового створення користувачів.

Доцільним є підхід, за якого система фіксує проблему, пропускає некоректний запис або позначає його як невдалий і продовжує роботу з наступними користувачами.

3.2. Алгоритм створення користувачів

Алгоритм створення користувачів у системі ADUserCreator побудований як послідовність етапів, які виконуються адміністратором та програмними модулями системи. Така структура дозволяє до початку створення облікового запису перевірити коректність вихідних даних, сформувати необхідні атрибути, визначити місце розміщення користувача в Active Directory та підготувати параметри доступу.

На першому етапі адміністратор запускає програму та завантажує Excel-файл із переліком користувачів. Система зчитує записи, перевіряє наявність необхідних полів, нормалізує текстові значення та готує дані до подальшої обробки. Після цього виконується транслітерація ПІБ і формування базових ідентифікаторів користувача.

На другому етапі система перевіряє унікальність сформованих логінів та поштових адрес у середовищі Active Directory. Якщо знайдено збіг, програма фіксує відповідне повідомлення в журналі та застосовує передбачений сценарій обробки. Такий підхід запобігає створенню дубльованих облікових записів.

На третьому етапі адміністратор обирає цільовий OU і групи доступу. Ці параметри визначають, де саме в структурі домену буде створений користувач і які права або ресурси він отримає після створення. Після підтвердження параметрів система переходить до виконання операцій у Active Directory.

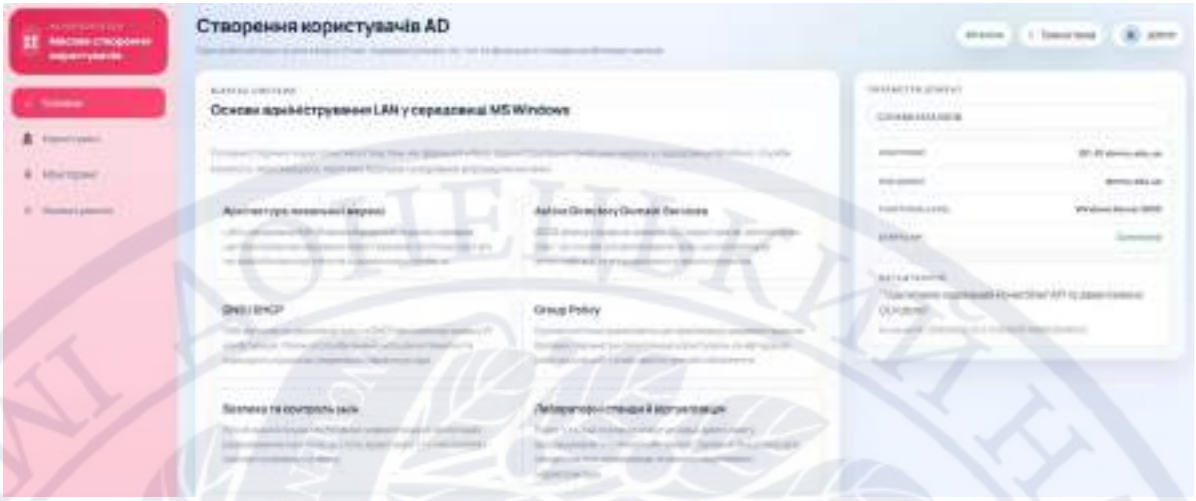

Рисунок 3.4 - Процес створення користувачів Active Directory.

На четвертому етапі система створює обліковий запис користувача через модуль роботи з Active Directory. Для користувача встановлюються основні атрибути: ім’я, логін, UPN, електронна адреса, організаційний підрозділ та інші службові поля, необхідні для подальшого адміністрування.

Після створення облікового запису система додає користувача до вибраних груп доступу. Якщо додавання до певної групи завершується помилкою, подія фіксується в журналі, а адміністратор отримує можливість проаналізувати результат і повторити операцію вручну або після виправлення причини помилки.

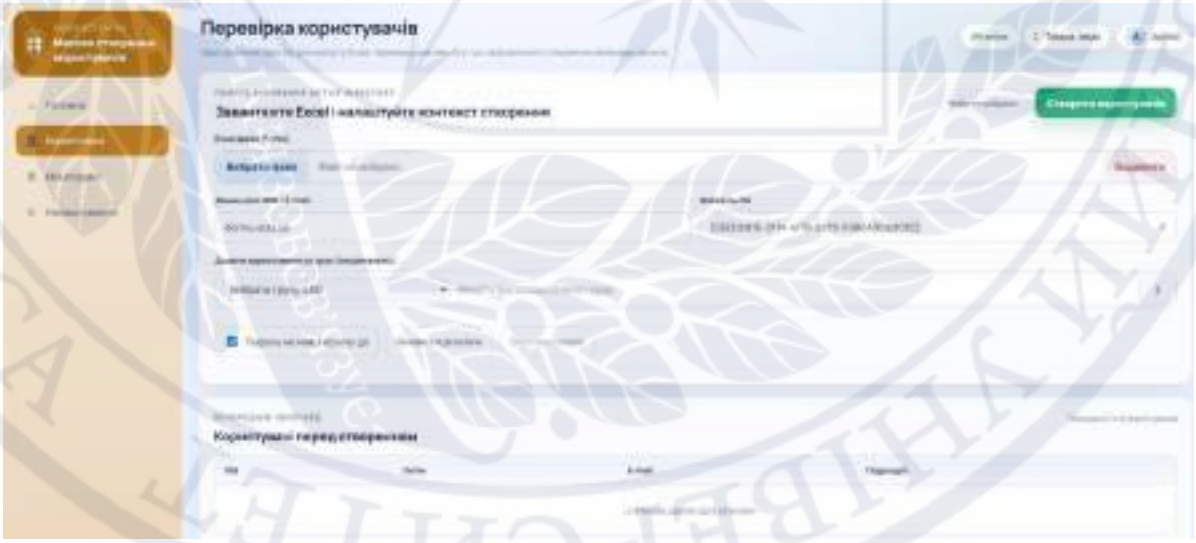

Рисунок 3.5 - Перевірка користувачів перед створенням.

Рисунок 3.6 - Перегляд створених облікових записів.

На наступному етапі система формує підсумкові результати виконання. Для кожного користувача зберігається статус операції, сформований логін, поштова адреса, службова інформація про створення та повідомлення про можливі помилки. Ці дані використовуються для формування звітності й контролю виконання.

Рисунок 3.7 - Оцінювання ефективності роботи програми.

Процес виконання операцій супроводжується моніторингом і журналюванням. Це дає змогу адміністратору бачити поточний стан обробки, кількість успішно створених користувачів, попередження та помилки. Такий механізм є важливим для масового створення облікових записів, оскільки дозволяє швидко визначити проблемні записи.

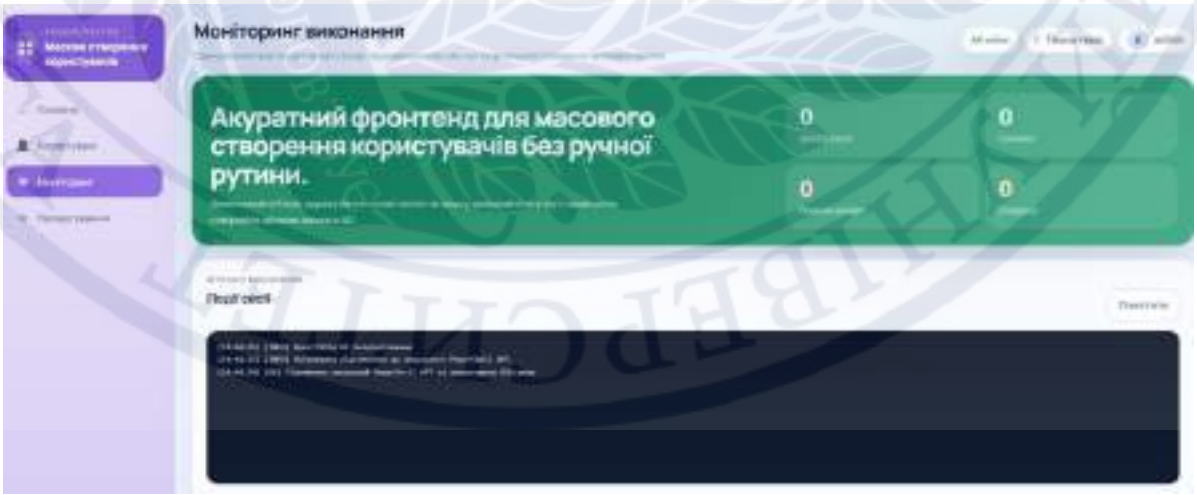

Рисунок 3.8 - Моніторинг виконання програми.

Додаткові параметри інтерфейсу дозволяють адаптувати роботу системи до конкретних умов доменної інфраструктури. Адміністратор може налаштовувати окремі параметри створення користувачів, вибору OU, груп доступу та формування службових атрибутів.

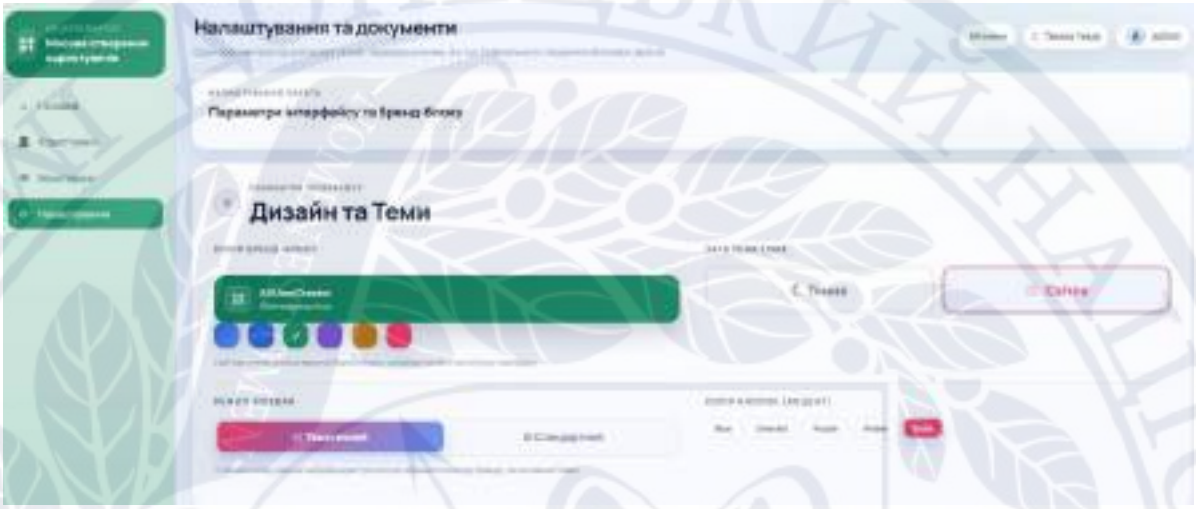

Рисунок 3.9 - Розширені можливості конфігурації інтерфейсу.

Завершальним етапом є формування PDF-файлу з обліковими даними та збереження журналу виконання. PDF-документ містить інформацію, необхідну для первинного входу користувача, а журнал дозволяє адміністратору підтвердити результат виконання операцій.

Рисунок 3.10 - Журнал паролів користувачів.

Отже, алгоритм роботи ADUserCreator охоплює повний цикл автоматизованого створення користувачів: від імпорту вихідних даних до формування облікових записів, додавання до груп, підготовки PDF-файлу та фіксації результатів у журналі.

3.3. Візуальне відображення результатів розробки за допомогою UML

Для формалізованого опису структури та поведінки системи використано UML-діаграми. Вони відображають основні варіанти використання, послідовність виконання алгоритму, взаємодію програмних модулів і загальну компонентну структуру системи.

Діаграма варіантів використання показує основні дії адміністратора: імпорт Excel-файлу, вибір OU, вибір груп, створення користувачів, формування PDF-файлу та перегляд журналу виконання.

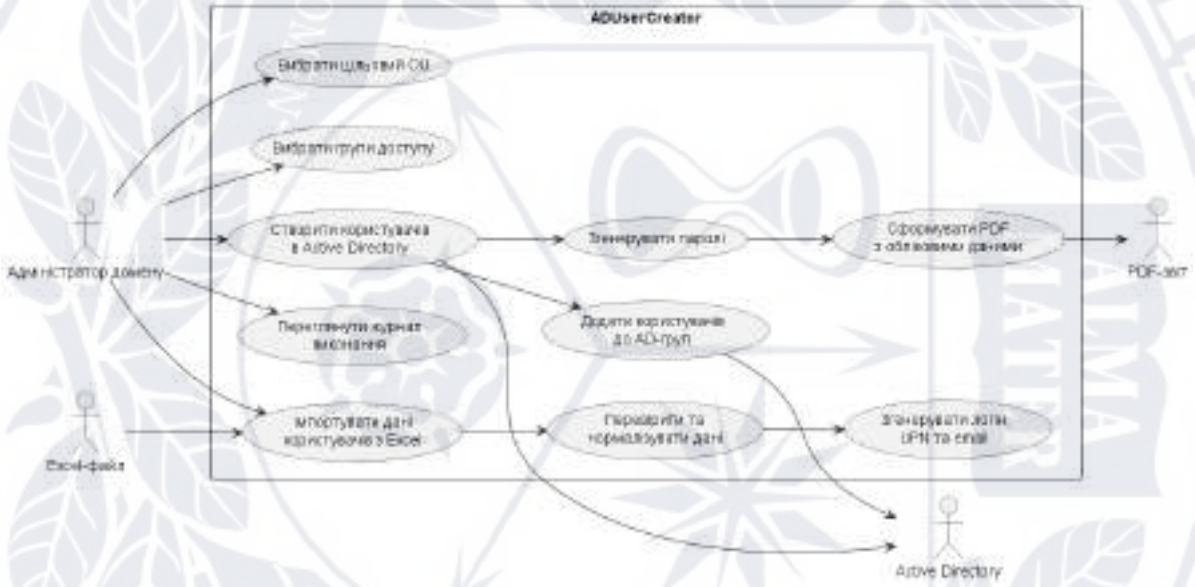

Рисунок 3.11 - Діаграма варіантів використання системи ADUserCreator.

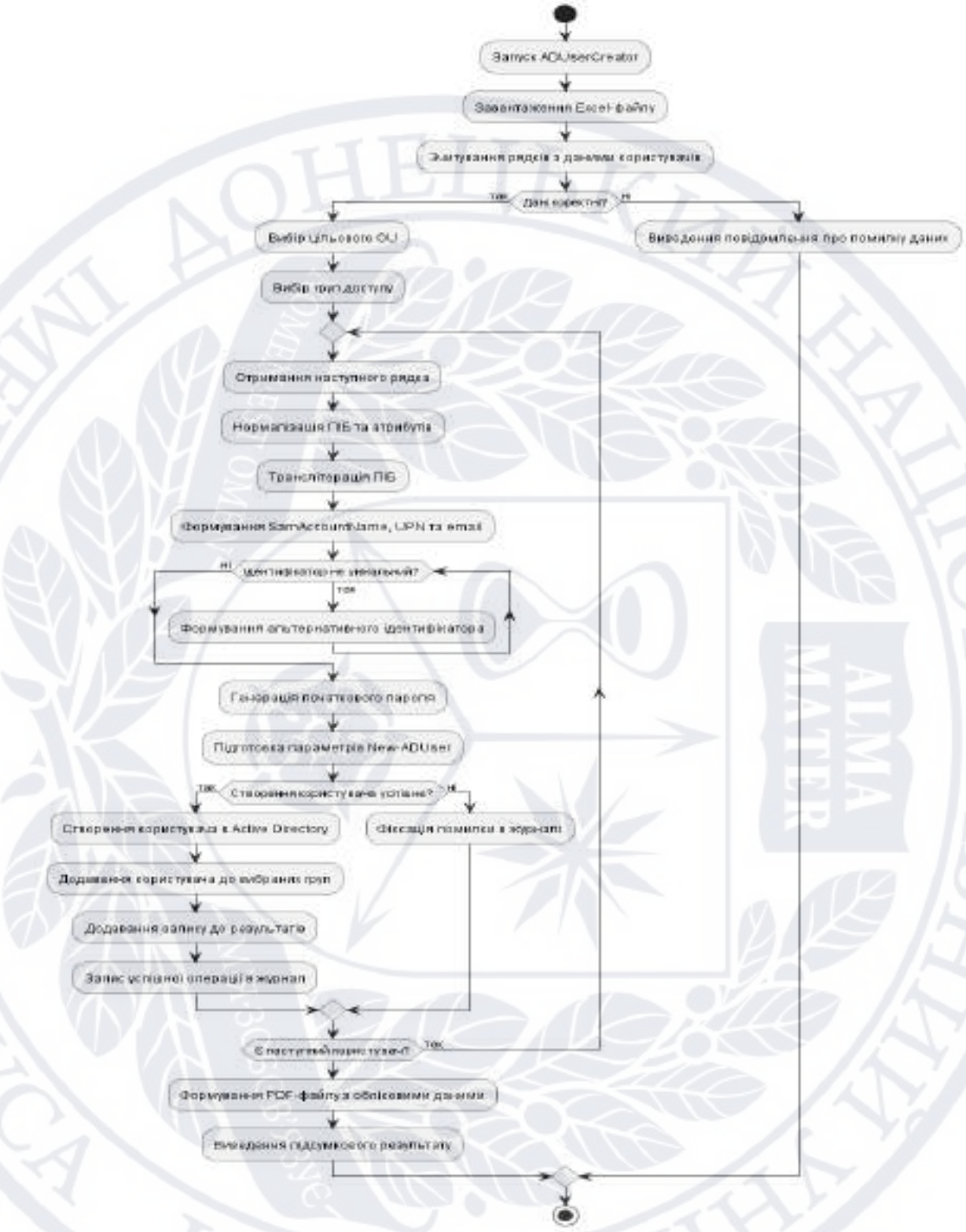

Рисунок 3.12 - Діаграма активності процесу створення користувачів.

Діаграма активності деталізує алгоритм створення користувачів від запуску програми до завершення обробки та формування результатів.

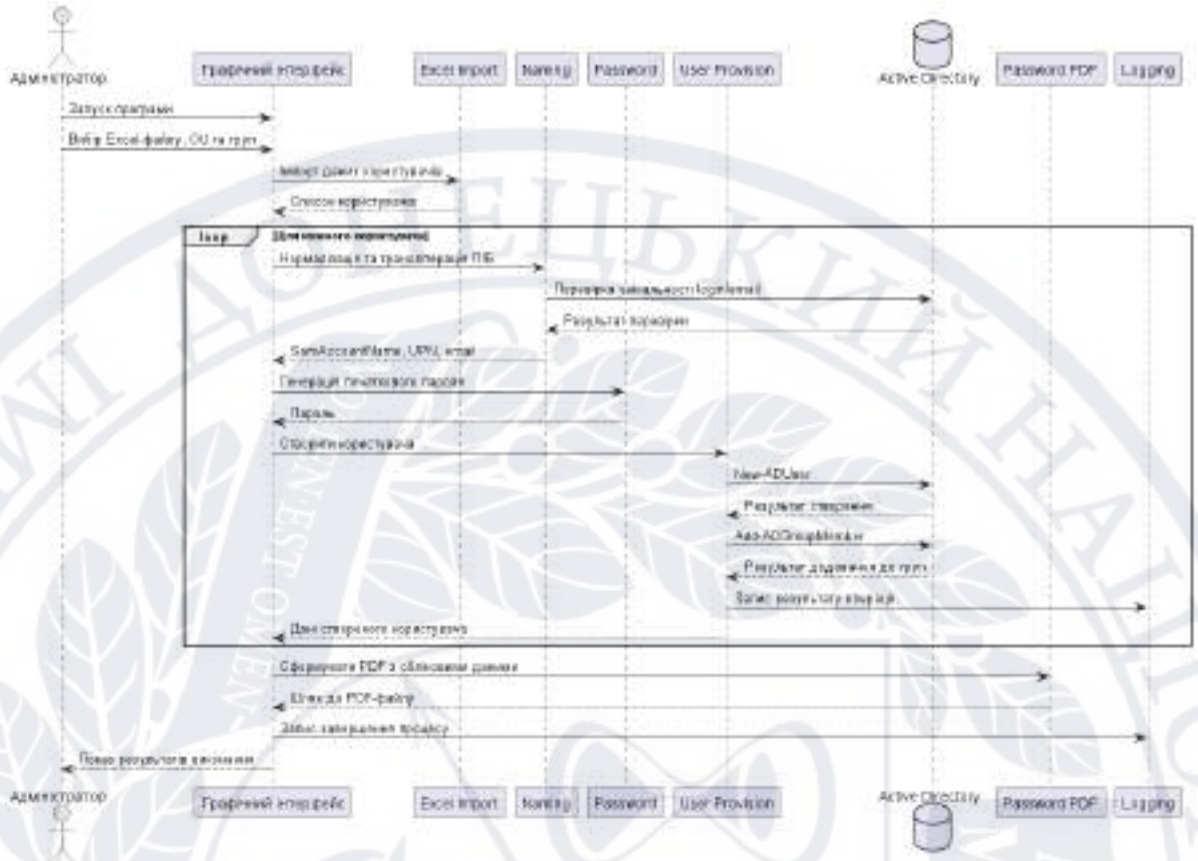

Рисунок 3.13 - Діаграма послідовності створення облікового запису.

Діаграма послідовності відображає обмін повідомленнями між адміністратором, графічним інтерфейсом, модулем імпорту, модулем генерації імен, Active Directory та PDF-модулем.

Таким чином, алгоритм системи побудований за принципом поетапної обробки даних із перевірками на ключових точках. Це підвищує надійність виконання операцій і дозволяє адміністратору контролювати процес на всіх етапах: від завантаження списку до отримання PDF-файлу та журналу результатів.

Контрольний етап включає фіксацію результатів, обробку помилок і формування підсумкових документів. Якщо певний запис не вдалося створити, система не повинна зупиняти всю обробку, а має зафіксувати проблему і перейти до наступного користувача. Такий підхід є важливим для масових операцій, коли помилка в одному рядку не повинна блокувати створення інших облікових записів.

Після створення облікового запису система переходить до призначення груп доступу. Цей етап є важливим, оскільки сам факт створення користувача ще не гарантує можливість працювати з потрібними ресурсами. Додавання до груп дозволяє відразу надати типовий набір прав, який відповідає ролі користувача або його підрозділу.

Виконавчий етап полягає в обробці кожного рядка вхідного файлу. Для кожного користувача система виконує нормалізацію ПІБ, транслітерацію, формування логіна, UPN та email, перевірку унікальності ідентифікаторів і генерацію початкового пароля. Після цього готуються параметри для створення об’єкта користувача в Active Directory.

Алгоритм роботи ADUserCreator можна розглядати як послідовність підготовчих, виконавчих і контрольних дій. Підготовчий етап охоплює запуск програми, вибір Excel-файлу, перевірку структури даних, вибір OU та груп доступу. На цьому етапі адміністратор визначає параметри, які будуть застосовані до всіх або частини користувачів.

Рисунок 3.14 - Діаграма компонентів системи ADUserCreator.

Діаграма компонентів демонструє внутрішню будову системи та взаємозв’язки між основними модулями: інтерфейсом користувача, імпортом Excel, генерацією ідентифікаторів, модулем створення користувачів, генератором паролів, PDF-модулем, журналюванням і модулем Active Directory.

Діаграма компонентів завершує опис архітектури, оскільки відображає внутрішню будову системи. Вона показує, що імпорт Excel, генерація ідентифікаторів, створення користувачів, формування паролів, PDF-документа та журналу виконання реалізуються як окремі логічні блоки. Такий розподіл спрощує супровід і створює основу для подальшого розвитку програмного продукту.

Діаграма послідовності деталізує обмін даними між компонентами під час виконання операції. Вона показує, які модулі викликаються першими, куди передаються результати перевірок і на якому етапі виконується взаємодія з Active Directory. Така модель допомагає перевірити, чи логічно розподілені обов'язки між частинами програми.

Діаграма активності є корисною для опису алгоритму, оскільки вона демонструє не тільки послідовність дій, а й точки прийняття рішень. У системі створення користувачів такими точками є перевірка коректності даних, перевірка унікальності логіна та результат виконання операції в Active Directory. Завдяки цьому діаграма показує як основний сценарій, так і можливі відхилення.

Діаграма варіантів використання дає змогу визначити, які саме дії виконує адміністратор і які зовнішні об'єкти беруть участь у процесі. Це допомагає уточнити функціональні межі системи: ADUserCreator відповідає за підготовку та запуск операцій, Active Directory - за зберігання й обробку об'єктів каталогу, а PDF-звіт - за представлення результатів.

UML-діаграми в роботі використовуються не як окремий декоративний матеріал, а як засіб формалізації проєктних рішень. Вони дозволяють перейти від текстового опису функцій до структурованої моделі, у якій чітко видно учасників процесу, межі системи, послідовність дій і взаємозв'язки між модулями.

Для навчального закладу автоматизоване створення користувачів має прикладне значення під час початку навчального року, оновлення груп, прийняття нових працівників або підготовки доступу до внутрішніх сервісів. У такі періоди кількість однотипних операцій суттєво зростає, тому використання

спеціалізованого інструмента дозволяє скоротити час підготовки облікових записів і зменшити навантаження на IT-відділ.

Важливим показником є також зручність використання для адміністратора. Якщо програма зменшує кількість ручних команд, але при цьому має складний або незрозумілий інтерфейс, її практична цінність знижується. Тому в ADUserCreator значна увага приділяється графічній формі, вибору параметрів через елементи інтерфейсу та зрозумілому відображенню результатів виконання.

Оцінювання результатів роботи системи доцільно здійснювати за кількома критеріями. Першим критерієм є швидкість створення користувачів у порівнянні з ручним виконанням аналогічних дій. Другим критерієм є кількість помилок, які виникають під час заповнення атрибутів і додавання до груп. Третім критерієм є повнота журналу виконання, оскільки саме він дозволяє підтвердити результат масової операції.

3.4. Перспективи розвитку системи

Основним предметом реалізації в межах цієї роботи є desktop-додаток ADUserCreator для автоматизованого створення користувачів Active Directory. Водночас архітектура системи може бути розширена додатковими сервісами, які підвищують зручність експлуатації та інтеграцію з інформаційним середовищем закладу.

Одним із можливих напрямів розвитку є веб-кабінет користувача на базі LDAP-автентифікації. Такий портал може використовувати Active Directory як джерело ідентичності, а локальну базу даних - для зберігання технічної інформації, журналу входів, налаштувань користувача та службових атрибутів. При цьому доступ має розмежовуватися за ролями: студент, співробітник, викладач, методист або адміністратор.

Іншим напрямом розвитку є інтеграція з внутрішніми академічними системами закладу, зокрема з АС Деканат або Oracle-базою даних. У такій моделі

Active Directory відповідає за автентифікацію та базову ідентичність, локальна база порталу зберігає технічні дані, а академічна система надає навчальні відомості: групу, факультет, освітню програму, форму навчання, курс, статус студента та реквізити студентського квитка.

Окрему увагу при розширенні системи необхідно приділити захисту з'єднань. Для веб-порталу доцільно використовувати HTTPS через Nginx, а для взаємодії з контролером домену - LDAPS або StartTLS з перевіркою сертифікатів. Такий підхід забезпечує захист облікових даних під час передавання мережею та відповідає базовим вимогам безпеки корпоративної інфраструктури.

Також можливе впровадження допоміжного AI-модуля як контрольованого консультативного шару над дозволеними API системи. Такий модуль не повинен мати доступу до паролів, конфіденційних файлів конфігурації або довільного виконання команд. Його доцільно використовувати для пояснення статусів синхронізації, підказок адміністратору та формування коротких довідкових відповідей на основі вже дозволених даних.

Інтеграцію з офіційними державними системами, зокрема ЄДЕБО, слід розглядати лише через офіційно надані канали доступу та погоджені механізми обміну даними. У межах цієї роботи такі модулі доцільно описувати як перспективу розвитку, не включаючи їх до основної логіки створення користувачів Active Directory.

Таким чином, розроблена система ADUserCreator може виступати ядром ширшої інфраструктури керування цифровими обліковими записами. Її подальший розвиток може охоплювати веб-інтерфейс, інтеграцію з академічними джерелами даних, захищені канали обміну, журнали аудиту та допоміжні інтелектуальні сервіси, але базовою функцією системи залишається автоматизоване створення користувачів Active Directory.

Попри можливі напрями розвитку, базова цінність системи полягає у стандартизації типового процесу створення користувачів. Якщо організація має чіткі правила іменування, структуру OU та групову модель доступу,

ADUserCreator дозволяє перетворити ці правила на повторюваний програмний процес. Це зменшує залежність результату від ручних дій адміністратора та підвищує якість супроводу доменної інфраструктури.

Можливим є також розвиток звітності. Крім PDF-файлу з початковими обліковими даними, система може формувати технічні звіти для адміністратора: список успішно створених користувачів, список помилок, статистику часу виконання, кількість оброблених записів і перелік груп, до яких були додані користувачі. Це підвищить прозорість роботи системи та спростить документування адміністративних операцій.

Ще одним напрямом розвитку є посилення механізмів безпеки. Доцільно передбачити розмежування доступу до функцій програми, додаткову перевірку прав адміністратора, контроль дій із підвищеним ризиком і захищене зберігання службових параметрів. Оскільки система працює з обліковими записами, вона повинна розглядатися як адміністративний інструмент, для якого важливі аудит і дотримання внутрішніх правил безпеки.

У перспективі ADUserCreator може бути доповнений механізмами інтеграції з іншими джерелами даних, однак такі розширення мають зберігати основний принцип системи - контрольоване створення користувачів у Active Directory. Наприклад, замість Excel-файлу джерелом може бути кадрова система, навчальна база або внутрішній портал, але логіка перевірки, формування ідентифікаторів, вибору OU та журналювання повинна залишатися обов’язковою.

Отже, ADUserCreator можна розглядати як приклад прикладного інструмента автоматизації, який побудований навколо реальної адміністративної потреби. Його цінність полягає в поєднанні можливостей PowerShell, графічного інтерфейсу, роботи з Excel, Active Directory, PDF-звітності та журналювання в одному контрольованому робочому процесі.

У результаті підвищується не лише швидкість виконання завдань, а й якість адміністрування. Наявність єдиних правил і журналу виконання спрощує перевірку результатів, дозволяє швидше знаходити помилки та формує основу

для подальшого розвитку системи. Це особливо важливо для організацій, де кількість користувачів регулярно змінюється.

Використання ADUserCreator дозволяє стандартизувати ті дії, які під час ручного виконання залежать від уважності адміністратора. Система не усуває потребу в контролі з боку фахівця, однак бере на себе повторювані технічні операції: обробку списку, формування ідентифікаторів, створення облікового запису, додавання до груп і підготовку звітних матеріалів.

З практичної точки зору розроблена система демонструє, що навіть відносно вузький адміністративний сценарій може мати значний вплив на ефективність роботи IT-підрозділу. Масове створення користувачів є типовою, але відповідальною операцією, у якій поєднуються вимоги до швидкості, точності, безпеки та документування результатів.

ВИСНОВКИ

У результаті виконання дипломної роботи було успішно реалізовано поставлену мету створено та обґрунтовано ефективне програмне рішення для автоматизації управління обліковими записами користувачів у корпоративному середовищі з використанням платформи Active Directory. Під час дослідження проведено детальний аналіз теоретичних основ управління обліковими записами в корпоративних інформаційних системах. Визначено ключові аспекти організації доступу до ресурсів, роль централізованих служб каталогів, а також важливість уніфікованих процесів адміністрування. Особливий акцент зроблено на вивченні функціональних можливостей та архітектурних характеристик Active Directory як інструмента для управління ідентифікацією користувачів і доступом до корпоративних мереж. Це дало змогу краще зрозуміти принципи роботи доменних структур, організаційних одиниць, груп безпеки та політик доступу.

У ході роботи виявлено основні недоліки традиційних методів управління обліковими записами, зокрема високу витратність часу, залежність від людського фактора, ризик допущення помилок і відсутність зручних механізмів централізованого контролю. На основі цих спостережень оцінено найсучасніші підходи до автоматизації, що включають застосування сценаріїв, інтеграцію з табличними даними та розробку спеціалізованих інтерфейсів програмування. На підставі аналізу сформовано вимоги до автоматизованої системи, серед яких: можливість масового створення облікових записів, попередня перевірка даних, інтеграція з існуючими інструментами, зручний інтерфейс користувача та забезпечення безпеки обробки конфіденційної інформації. У відповідь на ці вимоги спроєктовано архітектуру desktop-додатку, який підтримує взаємодію між користувацьким інтерфейсом і серверною частиною через API та використовує сценарії для безпосередньої роботи з Active Directory.

Практична частина проєкту передбачала реалізацію програмного забезпечення для автоматизації процесу створення облікових записів. Система дозволяє зручно обирати організаційні одиниці та призначати групи доступу. Реалізовано функції імпорту даних із файлів Excel, можливість попереднього перегляду і тестового запуску dry-run, що забезпечує додатковий контроль перед внесенням змін у систему. Також додано механізм моніторингу виконаних операцій і функцію генерації звітів у вигляді PDF-файлів із детальною інформацією про облікові записи.

Тестування виявило високу ефективність та працездатність розробленої системи. Використання програми значно скоротило час на виконання стандартних адміністративних завдань, суттєво зменшило можливість помилок і підвищило комфортність роботи для IT-фахівців. У різноманітних сценаріях від одиничного створення облікових записів до масового їх додавання система демонструвала стабільну продуктивність і надійність.

Запропонована автоматизована система є перспективним рішенням для впровадження в корпоративному середовищі, адже вона значно спрощує процес адміністрування, забезпечує централізований контроль, знижує ймовірність помилок і сприяє оптимізації бізнес-процесів, пов’язаних із управлінням користувачами. Подальший розвиток системи може включати розширення її функціональних можливостей, інтеграцію з іншими сервісами управління ідентифікацією, а також вдосконалення механізмів безпеки та аудиту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Active Directory. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Active_Directory (дата звернення: 15.06.2026).
2. Групова політика Windows. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Групова_політика (дата звернення: 15.06.2026).
3. Електронний архів НУ «Львівська політехніка». IT-інфраструктура підприємств. URL: https://ena.lpnu.ua (дата звернення: 15.06.2026).
4. Кібербезпека в Україні. Державна служба спеціального зв'язку України. URL: https://cip.gov.ua (дата звернення: 15.06.2026).
5. Коваленко І. В. Адміністрування комп'ютерних мереж. URL: https://www.dut.edu.ua (дата звернення: 15.06.2026).
6. Національний інститут стандартів України. Стандарти інформаційної безпеки. URL: https://uas.gov.ua (дата звернення: 15.06.2026).
7. Політики безпеки інформаційних систем. Центр кіберзахисту України. URL: https://cert.gov.ua (дата звернення: 15.06.2026).
8. Портал IT-Expert Україна. Серверні технології. URL: https://itexpert.org.ua (дата звернення: 15.06.2026).
9. Сервер (обчислювальна техніка). Вікіпедія. URL: https://uk.wikipedia.org/wiki/Сервер (дата звернення: 15.06.2026).
10. Microsoft Learn. Active Directory Domain Services. URL: https://learn.microsoft.com/windows-server/identity/ad-ds/ (accessed: 15.06.2026).
11. Microsoft Learn. Group Policy Management. URL: https://learn.microsoft.com/windows-server/group-policy (accessed: 15.06.2026).
12. Microsoft Learn. Windows Server Documentation. URL: https://learn.microsoft.com/windows-server/ (accessed: 15.06.2026).
13. Inno Setup Downloads (JR Software). URL: https://jrsoftware.org/isdl.php#issrc (дата звернення: 15.06.2026).
14. Автоматизовані системи управління: навч. посіб. / Д. О. Дьомін, П. С. Пензєв. – Харків :ТОВ "ТЕХНОЛОГІЧНИЙ ЦЕНТР ГРУП", 2024. – 130 с.
15. Інформаційні та автоматизовані системи управління. Настанова. — Київ:«Центр учбової літератури», 2024. — 38 с.
16. Посібник з лекцій з дисципліни «Автоматизовані системи керування

технологічними процесами» / Укладач : Карташов В.В. – Тернопіль : Вид-во ТНТУ імені Івана Пулюя, 2017 – 149 с.

17. 9 НАЙКРАЩИХ інструментів керування Active Directory (2026) URL: https://www.guru99.com/uk/active-directory-management-reporting-tools.html (дата звернення: 12.05.2026)

18. Active Directory: фундамент корпоративної інфраструктури, який став головною ціллю атак URL: https://iitd.ua/active-directory-fundament-korporativnoi-infrastrukturi/ (дата звернення: 15.05.2026)

19. Посібник з Active Directory для початківців URL: https://corewin.ua/blog/active-directory-delegation-tutorial-for-beginners/ (дата звернення: 15.05.2026)

20. Романенко А. І. Безпека комп'ютерних систем. URL: https://www.kpi.ua (дата звернення: 15.06.2026).

21. Петров С. М. Інформаційні системи та мережі. URL: https://www.knuba.edu.ua (дата звернення: 15.06.2026).