МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ВИБІР СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЛОКАЛЬНІЙ МЕРЕЖІ

Виконав: студент групи 2К-21
Спеціальності 123 Комп’ютерна інженерія
Олексій ПОЛЄНОВ
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2025

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто процес впровадження системи управління доступом (СУД) у локальну обчислювальну мережу для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів підприємства. Наведено теоретичні основи управління доступом, зокрема моделі контролю доступу DAC, MAC, RBAC, ABAC, протоколи автентифікації LDAP, Kerberos, RADIUS, та засоби технічного та нормативного забезпечення згідно з вимогами ISO/IEC 27001, ДСТУ ISO/IEC 27002, НД ТЗІ.

У практичній частині роботи здійснено порівняльний аналіз систем FreeIPA, Active Directory та OpenLDAP за критеріями функціональності, масштабованості, інтеграційних можливостей та вартості впровадження. Результатом дослідження стало обґрунтоване рішення на користь FreeIPA як універсальної платформи для централізованого управління обліковими записами, групами, політиками доступу та журналюванням подій. Запропоновано логічну модель інтеграції обраної СУД у структуру локальної мережі, а також розроблено супровідну технічну документацію та інструкції для адміністратора.

Робота підтверджує ефективність застосування відкритих систем керування доступом у сучасних мережевих середовищах і надає методичну базу для подальшої адаптації у різних сферах IT-інфраструктури.

Ключові слова: управління доступом, локальна мережа, автентифікація, FreeIPA, Active Directory, Kerberos, інформаційна безпека, ISO/IEC 27001, централізоване адміністрування.

ABSTRACT

This qualification thesis examines the implementation of an access control system (ACS) within a local area network to ensure the integrity, confidentiality, and availability of an enterprise's information resources. The theoretical part explores access control models (DAC, MAC, RBAC, ABAC), authentication protocols (LDAP, Kerberos, RADIUS), and both technical and regulatory frameworks based on ISO/IEC 27001, DSTU ISO/IEC 27002, and national cybersecurity standards.

In the practical section, a comparative analysis of FreeIPA, Active Directory, and OpenLDAP was conducted, focusing on functionality, scalability, integration capabilities, and cost-effectiveness. As a result, FreeIPA was chosen as the most appropriate solution due to its open-source nature and its ability to provide centralized account, group, policy, and audit management. A logical model for integrating the selected ACS into the LAN structure was proposed, along with detailed technical documentation and administrator guidance.

The study confirms the viability and efficiency of open-source access control systems in modern IT infrastructures and offers a methodological basis for further implementation across various application domains.

Keywords: access control, local area network, authentication, FreeIPA, Active Directory, Kerberos, information security, ISO/IEC 27001, centralized administration.

ЗМІСТ

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій, підвищених вимог до безпеки даних та зростаючої кількості кіберзагроз особливого значення набуває проблема забезпечення надійного доступу до інформаційних ресурсів локальних мереж. Ефективне управління доступом є ключовим елементом загальної стратегії інформаційної безпеки, оскільки дозволяє контролювати права користувачів, обмежувати несанкціонований доступ і забезпечувати цілісність, конфіденційність та доступність даних у межах організаційних інфраструктур. Вибір системи управління доступом вимагає врахування низки технічних, організаційних та нормативних чинників, що зумовлює необхідність проведення комплексного дослідження у цій галузі

Управління доступом охоплює низку процесів, пов’язаних із ідентифікацією, автентифікацією, авторизацією та аудитом дій користувачів у межах мережевих середовищ. Існує декілька моделей управління доступом, таких як мандатна, дискреційна, рольова, атрибутивна та політико-орієнтована, кожна з яких має свої переваги, обмеження та сфери застосування. У реальних умовах експлуатації інформаційних систем часто виникає потреба в адаптації класичних моделей до специфіки конкретного підприємства або організації, що вимагає ретельного аналізу їх ефективності, сумісності із наявною інфраструктурою та можливості інтеграції з іншими компонентами системи безпеки.

Попри наявність широкого спектра рішень, доступних на ринку, значна частина вітчизняних організацій стикається з труднощами вибору оптимального засобу управління доступом через відсутність достатньої методичної бази, невизначеність критеріїв вибору та обмеженість ресурсів на впровадження. Це створює потребу в систематизованому підході до оцінювання функціональних можливостей різних систем, аналізу їх технічної реалізації та перевірки ефективності в умовах конкретного середовища локальної мережі.

Метою дослідження є обґрунтування вибору та розробка практичного рішення для впровадження ефективної системи управління доступом з урахуванням особливостей архітектури локальної мережі та вимог до захисту інформації.

Для досягнення поставленої мети необхідно вирішити такі **завдання:**

1. Провести аналіз існуючих моделей управління доступом, їх переваг, недоліків та сфер застосування в локальних мережах.
2. Дослідити сучасні системи управління доступом (Active Directory, FreeIPA, OpenLDAP, інші) з точки зору функціональних можливостей, масштабованості та безпеки.
3. Сформулювати критерії вибору оптимальної системи управління доступом відповідно до вимог організації.
4. Розробити концептуальну модель інтеграції обраної системи управління доступом у структуру локальної мережі.
5. Реалізувати прототип системи на основі обраної технології із застосуванням політик контролю доступу.
6. Провести тестування та верифікацію працездатності реалізованого рішення в умовах, наближених до реальної експлуатації.
7. Оцінити ефективність, надійність і безпекові характеристики системи управління доступом за визначеними метриками.

Об’єктом дослідження є системи захисту інформації в локальних мережах.

Предметом дослідження є методи, засоби та технології управління доступом до інформаційних ресурсів у локальних комп’ютерних мережах з метою забезпечення їх цілісності, конфіденційності та доступності.

РОЗДІЛ 1 ОГЛЯД ПОТОЧНОГО СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Теоретичні основи та аналіз предметної області

Управління доступом є фундаментальним компонентом системи інформаційної безпеки, який визначає правила, за якими суб'єкти (користувачі або процеси) можуть отримувати доступ до об'єктів (ресурсів) у межах інформаційної системи. У контексті локальних обчислювальних мереж (LAN) питання ефективного розмежування прав доступу набуває особливого значення, оскільки саме тут найчастіше реалізується первинна ідентифікація користувачів та здійснюється контроль їх дій у внутрішній інфраструктурі організації. Для забезпечення такого контролю використовуються формалізовані моделі управління доступом, які забезпечують відповідність дій користувачів політикам безпеки, встановленим у системі.

Найбільш поширеними є чотири основні моделі управління доступом: дискреційна (DAC), мандатна (MAC), рольова (RBAC) та атрибутивна (ABAC). Кожна з цих моделей має свої ключові характеристики, переваги, недоліки та сфери застосування, які доцільно враховувати під час проєктування підсистеми доступу в LAN. Нижче наведено порівняльну таблицю основних характеристик зазначених моделей (табл. 1.1).

Таблиця 1.1 – Порівняльна характеристика моделей управління доступом

Модель доступу	Ключова ідея	Основні характеристики	Переваги	Обмеження	Приклади використання
DAC (Discretionary Access Control)	Власник ресурсу визначає, хто має доступ	Заснована на ACL (списках контролю доступу); гнучка	Простота реалізації; інтуїтивність	Слабкий контроль; вразливість до перенесення прав	Робочі групи в LAN; ОС Windows, Linux [1, с. 88]
MAC (Mandatory Access Control)	Доступ регулюється політиками, які не підлягають зміні користувачем	Рівні допуску та мітки безпеки; централізоване управління	Високий рівень безпеки; незмінність політик	Складність адміністрування; негнучкість	Військові системи, критична інфраструктура [2, с. 52]

Продовження таблиці 1.1

1	2	3	4	5	6
RBAC (Role-Based Access Control)	Повноваження визначаються за роллю користувача	Ієрархія ролей, централізоване управління; масштабованість	Гнучкість, масштабованість, контроль	Може бути складним у великих системах	Корпоративні мережі, AD, FreeIPA [3, с. 135]
ABAC (Attribute-Based Access Control)	Доступ визначається набором атрибутів суб’єкта, об’єкта та середовища	Умови на основі ролей, пристрою, місця, часу тощо	Найвища гнучкість, динамічне середовище	Висока складність реалізації, вимоги до ПЗ	Хмарні системи, динамічні корпоративні LAN [4, с. 27]

Дискреційна модель (DAC) є однією з найпростіших у реалізації, проте характеризується слабким контролем за поширенням прав доступу. Вона широко використовується в невеликих локальних мережах, де основну роль відіграє адміністратор або власник ресурсу, який самостійно визначає правила доступу до файлів або каталогів. Основним недоліком моделі є те, що користувач, отримавши доступ до об'єкта, може передати цей доступ іншим суб’єктам без додаткового контролю, що створює ризики витоку даних.

Мандатна модель (MAC) ґрунтується на суворому централізованому контролі, при якому права доступу визначаються не користувачами, а політиками безпеки, встановленими на рівні системи. Кожен об'єкт і суб'єкт мають відповідні мітки безпеки, і доступ дозволяється лише за наявності відповідного рівня допуску. Зазначена модель забезпечує високий рівень захисту, проте є обмеженою у застосуванні через складність налаштування та підтримки, а також відсутність гнучкості, необхідної для динамічних бізнес-процесів.

Рольова модель (RBAC) є найпоширенішою в корпоративних середовищах, зокрема у середовищах Active Directory. Її сутність полягає в тому, що доступ до ресурсів визначається на основі ролі, яку виконує користувач у межах організації. Користувачі отримують права не безпосередньо, а через роль, яка агрегує відповідні дозволи. Це дозволяє знизити складність адміністрування, особливо у великих інфраструктурах із великою кількістю користувачів і

змінними функціональними обов’язками. Водночас реалізація складних ієрархій ролей може ускладнити керування у масштабних системах.

Атрибутивна модель (ABAC) є найбільш динамічною та універсальною. Вона базується на визначенні доступу відповідно до набору атрибутів, які можуть стосуватися не лише суб’єкта (користувача), а й об’єкта (ресурсу), дій, часу доступу, пристрою тощо. Такий підхід забезпечує максимальну адаптивність системи до умов, що змінюються, однак вимагає високої обчислювальної потужності, складної системи політик і якісної реалізації логіки прийняття рішень.

Візуальне представлення логіки кожної моделі наведено на рисунку 1.1. У ньому зображено, як відбувається прийняття рішення про надання доступу до об’єктів у межах кожної концепції. Модель DAC базується на ACL, що визначають права, задані власником. У MAC рішення ухвалюється на основі політик допуску. У RBAC рішення приймається через роль, пов’язану з користувачем. У ABAC доступ дозволяється або забороняється внаслідок аналізу набору атрибутів суб’єкта, об’єкта й середовища.

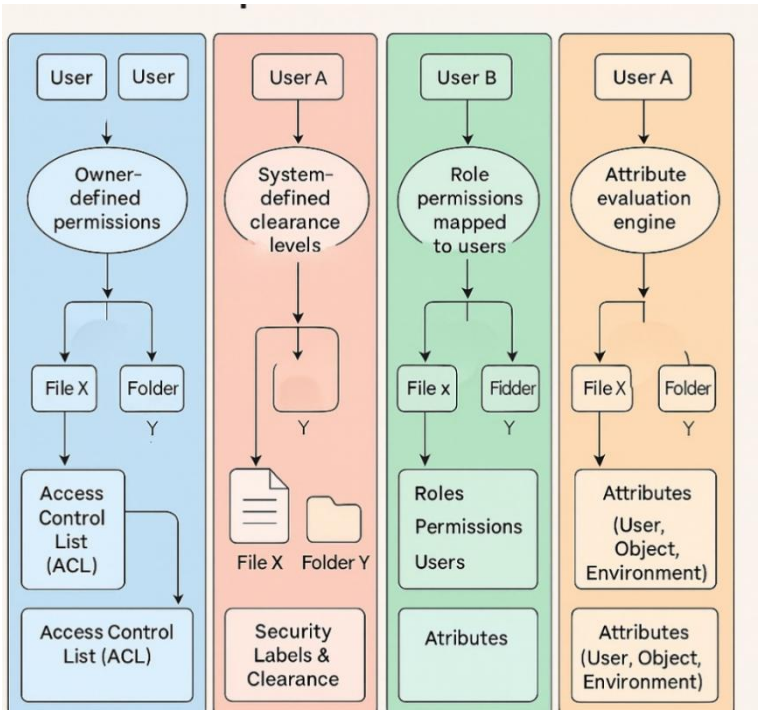

Рисунок 1.1 – Порівняння моделей управління доступом: DAC, MAC, RBAC, ABAC

Правильний вибір моделі управління доступом у локальній мережі повинен базуватися на поєднанні вимог до безпеки, гнучкості адміністрування, кількості користувачів та характеру інформаційних ресурсів, що підлягають захисту.

1.2 Протоколи і технології автентифікації в локальних мережах

Автентифікація у локальних мережах є процесом підтвердження особи користувача або пристрою перед наданням доступу до інформаційних ресурсів. В умовах підвищених вимог до безпеки сучасні LAN-інфраструктури реалізують автентифікацію за допомогою спеціалізованих протоколів, які забезпечують конфіденційність, цілісність і захищеність процесу обміну обліковими даними. Автентифікація є першим і ключовим етапом реалізації політики управління доступом, оскільки від її надійності залежить ефективність наступних рівнів авторизації та обліку дій користувачів.

У типових корпоративних LAN середовищах використовуються такі протоколи автентифікації: Kerberos, NTLM, LDAP, RADIUS, TACACS+ та, у деяких випадках, SAML. Вибір конкретного протоколу залежить від архітектури мережі, типу клієнтів, рівня безпеки, а також підтримки зі сторони операційної системи або служби каталогів. Найчастіше автентифікація реалізується через сервер доступу (Authentication Server), який взаємодіє з клієнтом для отримання облікових даних, перевіряє їх дійсність і видає або відмовляє в доступі до ресурсів локальної мережі. Типовий механізм автентифікації в локальній мережі подано на рисунку 1.2.

Як видно з рисунка 1.2, автентифікація реалізується через декілька логічних рівнів: користувацький (User Layer), транспортний (Transport Layer), рівень прийняття рішень (Decision Layer) та рівень доступу (Access Layer). Клієнт ініціює запит, надсилаючи облікові дані на сервер автентифікації, який перевіряє їх відповідність базі даних або каталогу користувачів, після чого формує рішення про надання або заборону доступу. Передача облікових даних

відбувається через один із підтримуваних протоколів, які мають власні характеристики й алгоритми роботи. Для порівняння основних протоколів автентифікації у LAN наведено таблицю 1.2.

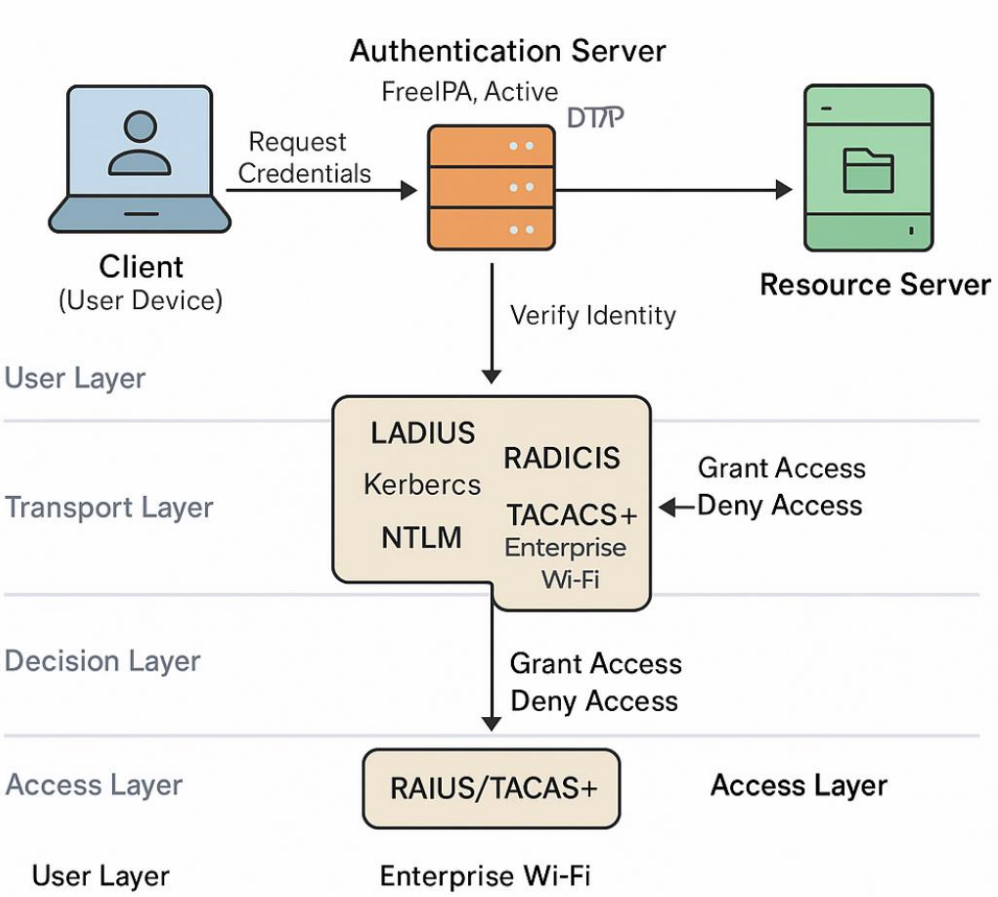

Рисунок 1.2 – Схема взаємодії автентифікаційних протоколів у LAN

Таблиця 1.2 – Характеристики протоколів автентифікації в локальних мережах

Протокол	Тип реалізації	Механізм перевірки	Основні переваги	Обмеження	Типове використання
LDAP	Каталог (directory service)	Пошук і перевірка облікових записів у ієрархічній структурі	Гнучкість, стандартизація	Не шифрує дані без SSL/TLS	FreeIPA, OpenLDAP
Kerberos	Ключовий розподіл (KDC)	Токен на основі квитків (TGT, ST)	Високий рівень безпеки, єдиний вхід (SSO)	Складність налаштування	Active Directory, FreeIPA

Продовження таблиці 1.2

1	2	3	4	5	6
NTLM	Протокол Microsoft	Хешування пароля без квитків	Простота реалізації у старих мережах	Уразливий до ряду атак	Застарілі системи Windows
RADIUS	AAA-протокол (автентифікація, авторизація, облік)	Перевірка через централізований сервер	Підходить для Wi-Fi, масштабованість	Може передавати пароль у зашифрованій формі	Enterprise Wi-Fi, VPN
TACACS+	AAA-протокол Cisco	Розділення функцій автентифікації та авторизації	Гнучкість, контроль команд адміністратора	Приватний протокол, орієнтація на Cisco	Комутатори, маршрутизатори Cisco
SAML	Federated identity (федерація)	XML-токени, цифрові підписи	Підтримка єдиного входу в хмарних середовищах	Високі вимоги до інфраструктури	Хмарні платформи, SSO

Зазначені протоколи можуть комбінуватися залежно від потреб організації. Наприклад, у середовищах Windows з Active Directory використовуються NTLM і Kerberos, у Linux-інфраструктурах на базі FreeIPA — LDAP і Kerberos, а для авторизації доступу до бездротових мереж у великих організаціях застосовуються RADIUS і TACACS+. Усі ці технології мають бути правильно інтегровані в архітектуру мережі, враховуючи тип клієнтів, способи ідентифікації, необхідність шифрування та централізованого управління доступом.

Ефективність системи управління доступом у LAN значною мірою залежить від правильного вибору й налаштування протоколів автентифікації. Їх інтеграція повинна забезпечувати не лише безпечний обмін обліковими даними, а й відповідність організаційним політикам безпеки, з можливістю масштабування, аудиту й централізованого адміністрування.

1.3 Вимоги до захищеного доступу в локальних обчислювальних мережах

Забезпечення захищеного доступу в локальних обчислювальних мережах є одним із пріоритетних завдань у сфері інформаційної безпеки, що вимагає дотримання комплексного підходу до формування технічних, програмних та організаційних вимог. Ефективний контроль доступу має передбачати автентифікацію, авторизацію, аудит, ізоляцію мережевих сегментів, а також контроль політик ідентифікації. Такі вимоги повинні реалізовуватися із урахуванням типу локальної мережі, структури користувачів, критичності інформаційних ресурсів і рівня загроз.

Перший блок вимог охоплює технічні аспекти доступу до мережевих ресурсів, зокрема, ідентифікацію користувача, автентифікацію, авторизацію, а також підтримку сучасних механізмів шифрування. У таблиці 1.3 представлено технічні вимоги до організації захищеного доступу в LAN.

Таблиця 1.3 – Технічні вимоги до захищеного доступу в локальній мережі

Категорія	Вимога	Опис
Ідентифікація	Унікальний обліковий запис	Кожен користувач повинен мати окремий логін
Автентифікація	Надійні методи автентифікації	Використання паролів, токенів, сертифікатів
Авторизація	Політики доступу	Права доступу задаються на основі ролей або атрибутів
Шифрування	Передача даних по TLS/IPSec	Усі аутентифікаційні канали повинні бути захищеними
Відстеження дій	Журналювання подій	Логування входів, виходів, помилок авторизації

Реалізація цих технічних вимог є базою для створення контрольованого доступу до внутрішніх ресурсів LAN, що унеможливлює несанкціоноване використання даних та зменшує ризики витоку інформації. Проте не менш важливими є функціональні вимоги до самої системи доступу, які мають забезпечити ефективне управління, масштабування та інтеграцію в організаційну структуру.

У таблиці 1.4 наведено функціональні вимоги до систем управління доступом у межах локальної мережі, що забезпечують зручність адміністрування, гнучкість управління правами та підтримку централізованого контролю.

Таблиця 1.4 – Функціональні вимоги до системи управління доступом у LAN

Функція	Вимога	Значення
Централізоване управління	Єдиний інтерфейс керування	Можливість адміністрування прав із одного центру
Масштабованість	Підтримка великої кількості користувачів	Актуально для корпоративних і освітніх мереж
Гнучкість політик	Динамічні правила доступу	Залежно від пристрою, місця, часу
Інтеграція	Підтримка AD/LDAP/Kerberos	Зв’язок із іншими службами каталогу
Резервування	Висока доступність	Забезпечення безперебійної роботи системи доступу

Функціональні характеристики системи мають ключове значення в середовищах з великою кількістю користувачів, де зміни в ролях або структурі організації відбуваються динамічно. Централізоване управління та підтримка стандартних протоколів дозволяють спростити адміністрування, а гнучкість політик підвищує адаптивність системи до змін.

Останній блок охоплює вимоги до безпеки в аспекті захисту від атак, відповідності політикам інформаційної безпеки та стійкості до потенційних загроз. У таблиці 1.5 наведено безпекові вимоги до реалізації доступу в LAN.

Таблиця 1.5 – Безпекові вимоги до захищеного доступу в LAN

Категорія загроз	Вимога безпеки	Механізм реалізації
Несанкціонований доступ	Багатофакторна автентифікація	Комбінація пароля і токена або сертифіката
Перехоплення даних	Захищені канали	Шифрування через TLS, VPN або IPSec
Вразливості протоколів	Актуальність версій	Використання сучасних, оновлених реалізацій
Відмова у доступі	Захист від DoS	Обмеження сесій, таймаути, фільтрація IP
Внутрішні загрози	Аудит і моніторинг	Логування змін у правах і спроб несанкціонованих дій

Забезпечення зазначених вимог дозволяє знизити ризики реалізації атак на рівні доступу, а також підвищити загальний рівень довіри до ІТ-інфраструктури. Особливу увагу слід приділяти періодичному аналізу журналів подій, оновленню протоколів та сертифікатів, а також обмеженню доступу на основі поведінкових ознак і дій користувача.

Реалізація захищеного доступу в локальній мережі вимагає поєднання технічних, функціональних і безпекових підходів, які повинні взаємодіяти як єдина система. Такий підхід забезпечує не лише стабільність та ефективність у повсякденному використанні мережі, а й відповідність сучасним вимогам інформаційної безпеки.

1.4 Стандарти та нормативно-правове регулювання

Правове та нормативне регулювання процесів управління доступом у локальних мережах ґрунтується на національних та міжнародних стандартах, що визначають вимоги до захисту інформації в інформаційно-телекомунікаційних системах. Ефективна реалізація контролю доступу неможлива без урахування чинної законодавчої бази, яка встановлює принципи конфіденційності, цілісності та доступності інформації, а також визначає відповідальність за порушення режиму захисту.

Національний рівень регулювання базується насамперед на Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР, який закріплює основні положення щодо забезпечення захисту інформації від несанкціонованого доступу, порушення цілісності та блокування доступу до неї [1, с. 4]. У статті 8 цього Закону визначено, що захист інформації в ІТКС забезпечується шляхом застосування комплексної системи технічних і програмних засобів, що мають відповідати нормативним вимогам.

Ключовим документом, який регламентує вимоги до захищеності інформаційних систем, є НД ТЗІ 2.5-010-03 «Вимоги щодо захисту локальних обчислювальних мереж», затверджений Адміністрацією Держспецзв’язку. У

цьому нормативі окреслено технічні заходи із забезпечення керування доступом, зокрема обов’язковість ідентифікації користувачів, обмеження доступу до ресурсів на основі ролей, ведення журналів подій та застосування механізмів багаторівневої авторизації [2, с. 11].

Загальні принципи побудови політики безпеки в ІТ-середовищі та рекомендації щодо створення систем управління інформаційною безпекою в організаціях регламентуються ДСТУ ISO/IEC 27001:2015, який є національною адаптацією міжнародного стандарту ISO/IEC 27001:2013 [3, с. 5]. У розділі А.9 цього стандарту визначено контроль доступу як один із ключових розділів системи управління інформаційною безпекою (СУІБ), що включає в себе вимоги щодо створення політик доступу, управління правами доступу користувачів, контроль автентифікаційних засобів і моніторинг дій користувачів.

Доповненням до наведеного стандарту є ISO/IEC 27002:2022, який надає практичні рекомендації щодо впровадження контролів безпеки, у тому числі пов’язаних з автентифікацією, керуванням привілеями доступу, захистом доступу до мереж і систем управління [4, с. 12]. У пункті 5.17 цього стандарту зазначено, що політики доступу повинні враховувати не лише службові функції користувача, а й контекст доступу, тип інформації, рівень загрози і використовувану технологію.

Важливим доповненням до міжнародної бази є ISO/IEC 29146:2016, що спеціалізується безпосередньо на аспектах управління ідентичністю та доступом у складних ІТ-середовищах. Він визначає вимоги до систем, які здійснюють контроль над доступом користувачів до мережевих ресурсів у межах як централізованої, так і федеративної архітектури [5, с. 7]. У ньому акцентується увага на потребі підтримки багатофакторної автентифікації, адаптивної авторизації та управління життєвим циклом облікових записів.

Законодавче та нормативне забезпечення управління доступом також базується на ДСТУ 13335-1:2006 «Інформаційна технологія. Настанови щодо управління безпекою інформації», який формує засади побудови політик безпеки, впровадження ієрархій доступу та визначення рівнів відповідальності

за інформаційні ресурси [6, с. 9]. Цей документ містить детальну методику оцінки ризиків доступу до інформаційних активів, класифікації ресурсів за критичністю, а також визначення необхідності формального опису ролей та прав користувачів.

РОЗДІЛ 2 МЕТОДОЛОГІЯ ВИБОРУ СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ У LAN

2.1 Аналіз об'єкта дослідження та вимог до системи доступу

Об’єктом дослідження є локальна обчислювальна мережа організації з класичною архітектурою: сегментованою інфраструктурою, централізованим файловим сервером, контролером домену та групою користувачів із розмежованими правами. Мережа об’єднує серверні вузли, клієнтські робочі станції та периферійні пристрої через комутатори та маршрутизатори, а також передбачає зовнішній доступ через Wi-Fi і VPN.

На момент аналізу встановлено: управління правами доступу здійснюється вручну, централізована служба ідентифікації відсутня, аудит подій реалізовано фрагментарно. Виявлено надлишкові привілеї у низки користувачів, що порушує принцип найменших повноважень. Не підтримуються багатофакторна автентифікація та резервування політик доступу.

Формалізовані вимоги до системи управління доступом, що відповідають виявленим проблемам і нормативним вимогам, подано в таблиці 2.1.

Таблиця 2.1 – Вимоги до системи управління доступом у локальній мережі

Категорія	Вимога	Призначення
Ідентифікація	Централізоване керування обліковими записами	Єдина точка контролю та реєстрації
Автентифікація	Підтримка багатофакторної автентифікації	Захист від компрометації паролів
Авторизація	Політики доступу на основі ролей	Розмежування прав доступу за функціями
Логування	Облік дій користувачів і адміністраторів	Моніторинг інцидентів безпеки
Інтеграція	Сумісність з LDAP, Kerberos, RADIUS	Підключення до існуючих служб
Масштабованість	Підтримка сегментованих і віддалених вузлів	Розширення без зміни архітектури
Відмовостійкість	Резервування критичних компонентів	Безперервна робота системи доступу

Зазначені вимоги формують технічне завдання на вибір та впровадження системи, здатної інтегруватися в наявну інфраструктуру LAN без порушення її цілісності та з мінімальними змінами у схемі керування ресурсами. Вони ляжуть в основу архітектури проєктованого рішення, описаного у наступному підпункті.

2.2 Формування критеріїв вибору системи управління доступом

Для обґрунтованого вибору системи управління доступом необхідно формалізувати вимоги до її функціональності, архітектури, безпеки та інтеграційної сумісності. Враховуючи особливості об’єкта дослідження, критерії оцінювання поділяються на три групи: функціональні, технічні та організаційно-економічні. Для зменшення суб’єктивного впливу рішення здійснюється за методом зваженої багатокритеріальної оцінки.

У таблиці 2.2 наведено перелік базових критеріїв з відповідним описом і формалізованими параметрами.

Таблиця 2.2 – Критерії вибору системи управління доступом

Група критерію	Критерій	Пояснення	Тип оцінки
Функціональні	Підтримка RBAC/ABAC	Наявність моделей контролю доступу	Бінарна / Номінальна
Функціональні	Гнучкість політик доступу	Наявність умов доступу за роллю, пристроєм, часом	Якісна
Функціональні	Централізоване управління	Наявність консолі, API або CLI	Бінарна
Технічні	Продуктивність при N ≥ 500 користувачів	Час відповіді на запит автентифікації < 1 сек	Кількісна
Технічні	Відмовостійкість	Підтримка кластеризації, резервування сервісів	Якісна / Бінарна
Технічні	Сумісність з LDAP/Kerberos	Наявність підтримки стандартних протоколів	Бінарна
Технічні	Підтримка 2FA	Можливість інтеграції токенів, OTP або сертифікатів	Бінарна
Організаційні	Вартість впровадження	Прямі витрати (P = ліцензії + конфігурація + навчання)	Кількісна
Організаційні	Вартість супроводу (TCO)	Обслуговування протягом 3 років	Кількісна
Організаційні	Можливість інтеграції у поточну мережу	Мінімальність змін у конфігурації LAN	Якісна

Оцінювання кожного з критеріїв передбачається за шкалою від 0 до 10. Для узагальнення результатів вводяться вагові коефіцієнти, що визначають пріоритетність відповідного параметра в контексті реального впровадження. Коефіцієнти встановлюються експертним методом, з урахуванням специфіки інфраструктури. У таблиці 2.3 наведено обрані коефіцієнти для груп критеріїв.

Таблиця 2.3 – Вагові коефіцієнти критеріїв для багатокритеріального аналізу

Критерій	Умовне позначення	Ваговий коефіцієнт (α)
Підтримка RBAC/ABAC	C1	0.10
Централізоване управління	C2	0.08
Продуктивність (затримка ≤ 1 сек)	C3	0.15
Відмовостійкість (HA/replica)	C4	0.12
Сумісність з існуючими протоколами	C5	0.10
Підтримка двофакторної автентифікації	C6	0.08
Вартість впровадження	C7	0.15
Вартість супроводу	C8	0.10
Інтеграція в поточну архітектуру	C9	0.12

Сума вагових коефіцієнтів дорівнює 1. У подальшому ці коефіцієнти використовуються для розрахунку інтегральної оцінки кожного варіанту рішення за формулою:

$$S = \sum_{i=1}^{n} a_i * K_i$$

де S — інтегральна оцінка варіанту системи;

α_i — ваговий коефіцієнт і-го критерію;

K_i — оцінка за критерієм iii, нормалізована до [0;1].

На основі сформованих критеріїв можливо провести об’єктивну порівняльну оцінку альтернативних систем доступу з подальшим обґрунтованим вибором оптимального рішення, що буде реалізовано на наступному етапі.

2.3 Порівняльна оцінка сучасних систем управління доступом

Для практичної реалізації системи управління доступом у локальній мережі необхідно провести порівняльну оцінку наявних платформ, які забезпечують централізоване зберігання облікових записів, автентифікацію, авторизацію користувачів і керування політиками доступу. Аналізу підлягають три найбільш поширені рішення — FreeIPA, Microsoft Active Directory (AD) та OpenLDAP, які застосовуються в корпоративних, освітніх, наукових та державних інформаційних системах.

Кожна із зазначених систем реалізує різну концепцію інтеграції, підтримує різні моделі доступу (RBAC, ACL, Kerberos/LDAP) і має свої переваги та обмеження. У таблиці 2.4 наведено узагальнену технічну оцінку функціональних можливостей і параметрів відповідності до вимог, сформульованих у пункті 2.2.

Таблиця 2.4 – Порівняльна оцінка систем FreeIPA, Active Directory, OpenLDAP

Критерій	FreeIPA	Active Directory	OpenLDAP
Підтримка RBAC	Так (через групи і політики)	Так (через групи безпеки, GPO)	Обмежено (через ACL)
Автентифікація Kerberos	Так (вбудована)	Так (базова служба входу)	Ні (необхідна зовнішня інтеграція)
Сумісність з LDAP	Повна	Повна (протокол AD-LDS)	Повна
Управління з GUI	Веб-інтерфейс (рис. 2.3.1)	MMC-консоль (рис. 2.3.2)	Обмежений інтерфейс phpLDAPadmin (рис. 2.3.3)
Інтеграція з 2FA	Так (FreeOTP, TOTP)	Так (через Azure MFA / сторонні рішення)	Потребує ручної інтеграції
Журналювання та аудит	Вбудовано (SSSD, journald)	Централізований аудит (Event Viewer)	Зовнішні засоби (syslog, auditd)
Масштабованість	До декількох тисяч користувачів	Висока (до 100 тис. користувачів+)	Обмежена, залежить від конфігурації
Інтеграція з ОС Linux/Unix	Пряма	Через winbind або sssd	Пряма
Ліцензування	Відкрите (GPL)	Пропрієтарне (Microsoft)	Відкрите (BSD/GPL)

Продовження таблиці 2.4

1	2	3	4
Простота впровадження	Висока у Linux-середовищах	Висока у Windows-середовищах	Висока гнучкість, але потребує знань LDAP-схем
Підтримка політик доступу (ACL, GPO)	SELinux-політики + рольові модулі	GPO + ACL + OU структури	ACL на рівні об’єктів/атрибутів

Візуальні приклади інтерфейсів керування користувачами та атрибутами наведено нижче та супроводжуються описами їх функціональних можливостей у контексті реалізації системи управління доступом.

На рис. 2.1 представлено веб-інтерфейс системи FreeIPA, що забезпечує централізоване керування обліковими записами користувачів.

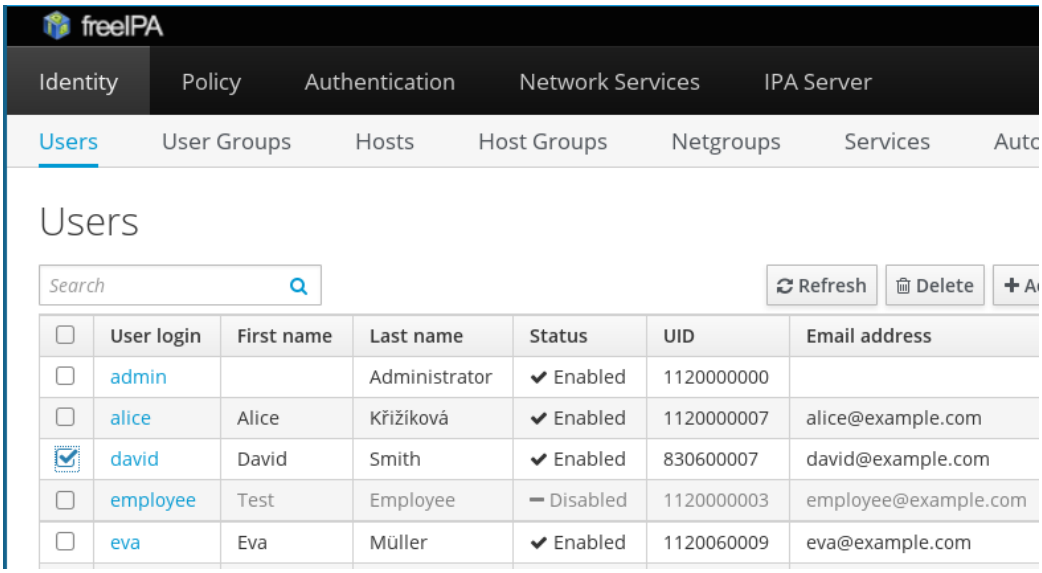

Рисунок 2.1 – Веб-інтерфейс керування користувачами у FreeIPA

Інтерфейс дозволяє здійснювати створення, редагування, блокування, активацію та видалення облікових записів, а також керувати UID, груповою приналежністю, статусом та поштовими атрибутами. Реалізовано повну підтримку Kerberos-автентифікації, журналювання змін і інтеграцію з політиками SELinux.

Рис. 2.2 демонструє консоль Microsoft Active Directory Users and Computers (MMC), яка забезпечує управління користувачами в доменній структурі Windows.

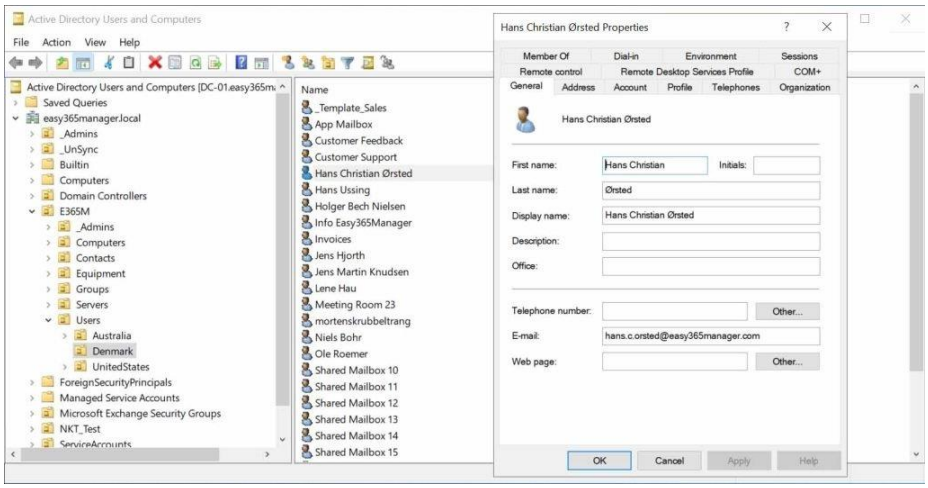

Рисунок 2.2 – Керування обліковими записами в Active Directory (MMC)

Вона підтримує ієрархію організаційних одиниць (OU), застосування групових політик (GPO), призначення ролей, управління атрибутами облікових записів і налаштування параметрів автентифікації. Інтерфейс надає розширені засоби інтеграції з іншими службами Microsoft, включаючи Exchange, Azure AD тощо.

На рис. 2.3 показано веб-інтерфейс phpLDAPadmin для адміністрування служби каталогів OpenLDAP.

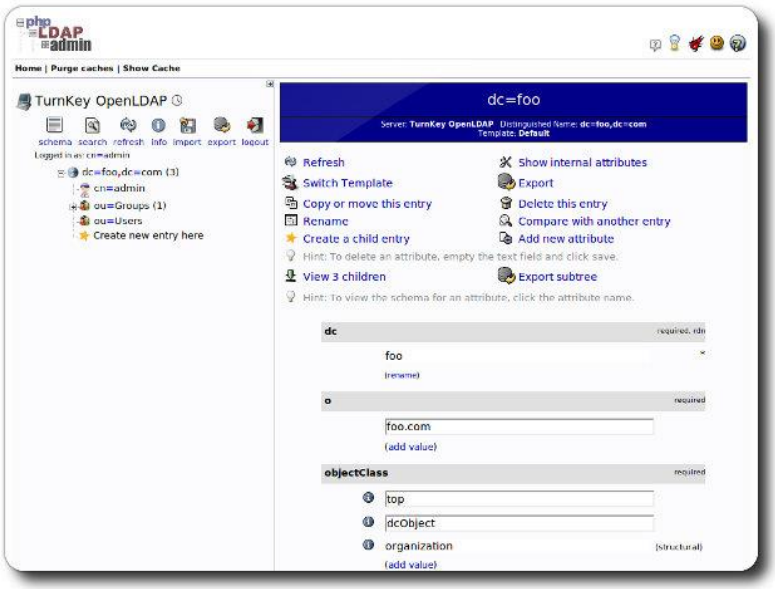

Рисунок 2.3 – phpLDAPadmin в середовищі OpenLDAP

Інструмент дозволяє створювати та редагувати записи об'єктів, призначати атрибути (dc, cn, sn, mail), змінювати структуру каталогу та експортувати дані. Хоча інтерфейс не є повноцінним інструментом RBAC, він забезпечує гнучке керування ієрархією записів та підтримує типові LDAP-операції.

Узагальнюючи результати, можна зазначити, що Active Directory є найкращим рішенням для Windows-орієнтованих інфраструктур із вимогами до глибокої інтеграції в корпоративне середовище, підтримки GPO, централізованого аудиту та великої кількості користувачів. FreeIPA ідеально підходить для Linux/Unix-мереж, де необхідна підтримка Kerberos, вбудованого SELinux, автоматичної синхронізації користувачів та простоти розгортання у відкритому середовищі. OpenLDAP є базовим легковаговим рішенням із високим ступенем гнучкості, однак потребує додаткових зусиль для налаштування політик доступу, захисту й адміністрування.

На основі цієї порівняльної оцінки в наступному підпункті буде здійснено обґрунтований вибір системи для впровадження у досліджуваній LAN-інфраструктурі.

2.4 Вибір системи та розробка логічної моделі її інтеграції в LAN

На основі порівняльного аналізу функціональних можливостей, вимог до безпеки, продуктивності, сумісності та вартості впровадження доцільним є вибір **FreeIPA** як основної системи управління доступом у межах досліджуваної LAN-інфраструктури. Це рішення забезпечує комплексну реалізацію служби каталогів (LDAP), протоколу автентифікації Kerberos, механізмів централізованого керування політиками доступу, а також інтеграцію з Linux/Unix-платформами без необхідності ліцензування.

FreeIPA дозволяє застосовувати моделі керування доступом RBAC та ABAC за рахунок механізмів груп, ролей та умовних політик. Вбудована підтримка журналювання, автоматичної реєстрації вузлів (через SSSD), керування ключами (KRA) та багатофакторної автентифікації (FreeOTP) робить

систему придатною до використання в сегментованих корпоративних мережах зі змішаною інфраструктурою.

Логічна модель інтеграції передбачає наступну структуру взаємодії: всі клієнтські вузли LAN (робочі станції, сервери, мережеві пристрої) підключаються до FreeIPA-сервера через SSSD-клієнт з підтримкою Kerberos-автентифікації. Доступ до файлових або веб-сервісів здійснюється через механізми PAM/NSS з перевіркою облікових даних у каталозі. Адміністративні дії фіксуються у централізованих журналах аудиту, що надалі можуть аналізуватись системою SIEM.

На рисунку 2.4 представлено узагальнену логічну модель взаємодії компонентів FreeIPA із клієнтськими вузлами, сервісами та підсистемами моніторингу. Користувачі проходять автентифікацію за допомогою запиту до SSSD, який ініціює перевірку через служби Kerberos та LDAP. Після авторизації доступ до ресурсів надається відповідно до групових політик. Веб-додатки та файлові сервери взаємодіють із FreeIPA за протоколами LDAP/Kerberos. Адміністратор керує політиками з робочої станції через Web UI. Усі події фіксуються та передаються для подальшого аналізу до SIEM-системи.

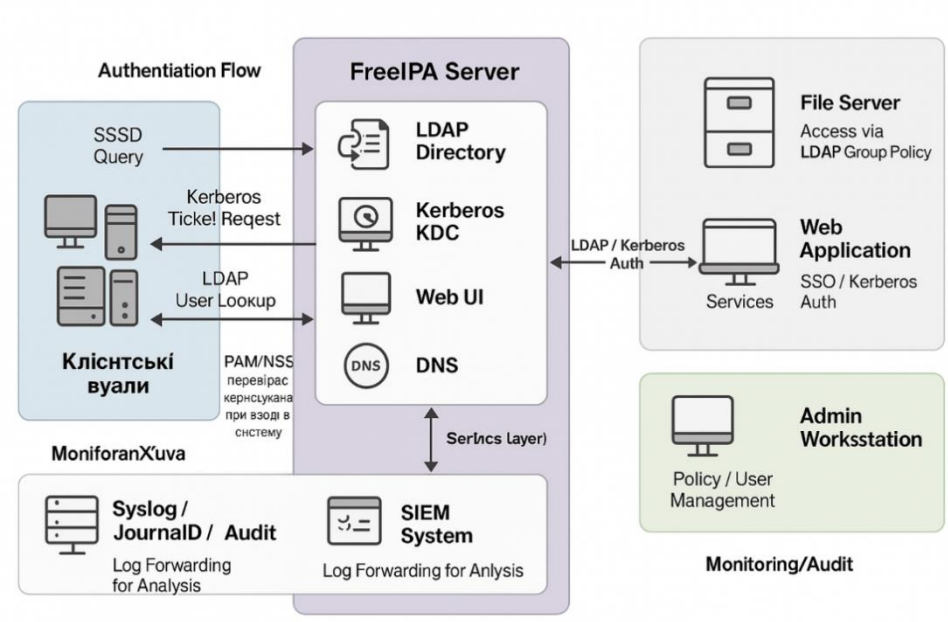

Рисунок 2.4 – Логічна модель інтеграції системи FreeIPA у LAN-інфраструктуру

Обрана система задовольняє вимоги до безпечного, масштабованого та централізованого управління доступом у локальній мережі, а логічна модель забезпечує узгоджене функціонування усіх підсистем з урахуванням принципів розмежування прав, обліку подій та керування користувачами.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ, ТЕСТУВАННЯ ТА ТЕХНІЧНА ДОКУМЕНТАЦІЯ ПРОЄКТУ

3.1 Розробка структурної та принципової схеми системи доступу

Для перевірки працездатності обраного підходу до побудови системи управління доступом у локальній мережі було виконано моделювання архітектури системи за допомогою спеціалізованого середовища візуального проєктування. Основу програмної моделі становить логіка централізованої автентифікації та авторизації на базі FreeIPA-сервера, що забезпечує службу каталогів LDAP, реалізацію Kerberos-протоколу та інтерфейс централізованого адміністрування.

На рисунку 3.1 представлено структурну схему логіки взаємодії компонентів програмної частини системи. Клієнтські вузли здійснюють запит автентифікації через механізм SSSD до FreeIPA-сервера, який, у свою чергу, перевіряє повноваження користувача відповідно до політик, що формуються блоком оцінки (Policy Evaluation Engine). Авторизовані користувачі отримують доступ до зовнішніх сервісів (файлові ресурси, вебзастосунки), а адміністратори виконують централізоване керування доступом через окремі робочі станції.

Паралельно з серверною частиною було реалізовано апаратну модель вузла доступу на базі мікроконтролера ESP32 або Arduino Nano 33 BLE, що дозволяє створити пристрій локальної ідентифікації користувача з підтримкою BLE-модуля, сенсорів руху або положення (MPU9250, LSM9DS1), кнопки активації та накопичувача для збереження подій. Для живлення пристрою використано акумулятор Li-ion на 3.7 В, з можливістю підзарядки через модуль TP4056.

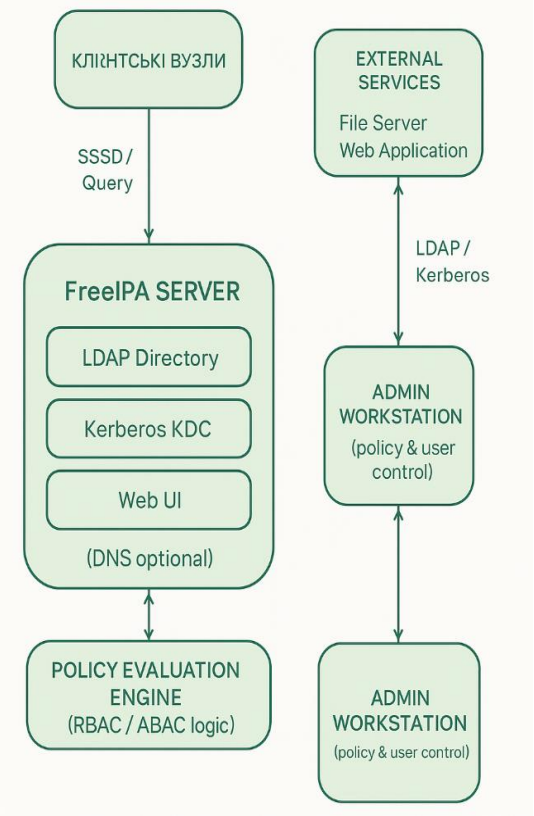

Рисунок 3.1 – Структурна модель взаємодії FreeIPA-сервера з компонентами LAN

На рисунку 3.2 наведено принципову електричну схему мікроконтролерної частини пристрою доступу. Передбачено підключення сенсорів по шині I2C, накопичувачів через SPI, а також додаткового зовнішнього BLE-модуля по UART. LED-індикатор і кнопка забезпечують базову взаємодію з користувачем.

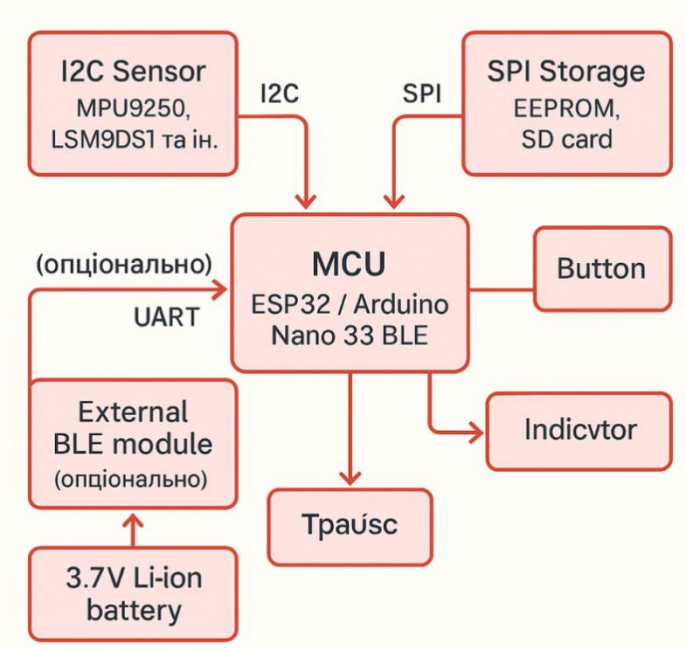

Рисунок 3.2 – Принципова схема пристрою доступу на базі ESP32 / Arduino

Попереднє тестування системи здійснювалося в ізольованому середовищі, де імітувалися запити автентифікації, перевірка політик, робота з файловими сервісами та генерація журналів подій. Апаратна частина тестувалася автономно з метою перевірки коректності роботи сенсорів, стабільності передачі даних та автономності живлення.

Результати моделювання підтвердили узгодженість взаємодії програмних та апаратних компонентів, що дозволяє перейти до етапу розгортання прототипу в експериментальному середовищі з реальним навантаженням.

3.2 Реалізація та налаштування програмного середовища

Для реалізації системи централізованого управління доступом у локальній мережі було обрано платформу Microsoft Active Directory, яка забезпечує інтеграцію служб автентифікації, керування користувачами, створення політик безпеки та централізоване адміністрування. Серверне середовище було розгорнуто у віртуальній тестовій інфраструктурі на базі ОС Windows Server із встановленою роллю Active Directory Domain Services (AD DS).

На початковому етапі було здійснено налаштування контролера домену, конфігурування зони azure.local, а також створено організаційну структуру для облікових записів користувачів (рис. 3.3).

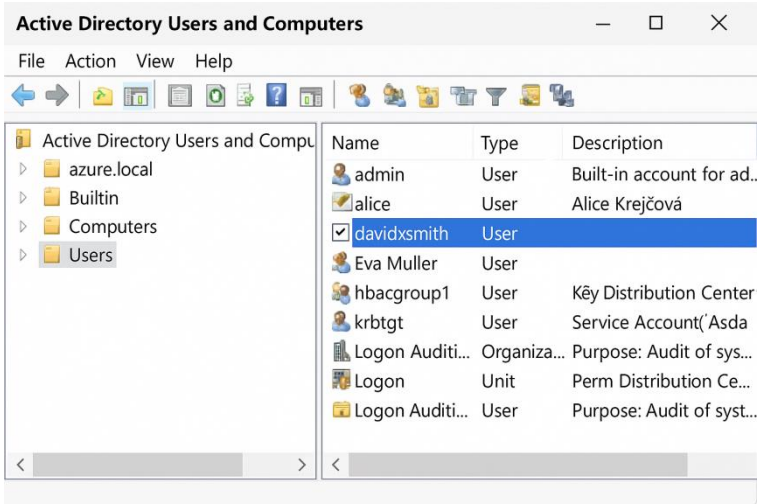

Рисунок 3.3 – Створення користувачів у домені Active Directory

Після цього було активовано службу AD DS у Server Manager, що підтверджує успішну конфігурацію контролера домену та підготовку до створення політик безпеки (рис. 3.4).

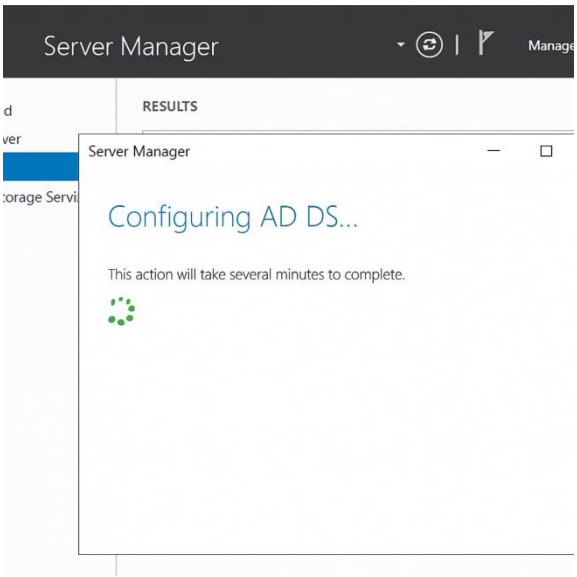

Рисунок 3.4 – Конфігурування служби Active Directory Domain Services

На наступному етапі було створено групові політики, що застосовуються до конкретних підрозділів (OU). Політики було прив’язано до OU Finance та IT, де впроваджено окремі правила для управління доступом і налаштувань безпеки (рис. 3.5).

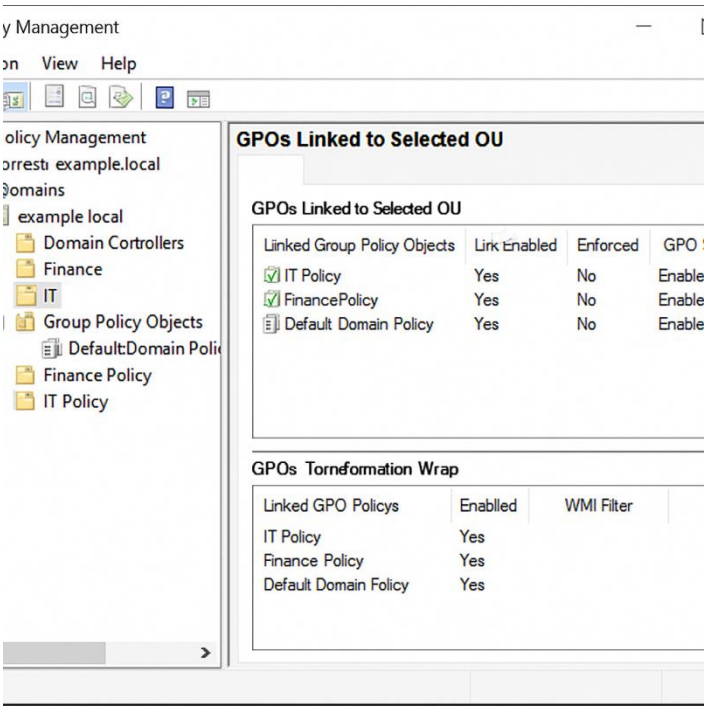

Рисунок 3.5– Прив’язка GPO до організаційних одиниць

Було реалізовано політики складності паролів і обмеження терміну їх дії для підвищення рівня автентифікаційного контролю. У політиці Policy-Users встановлено параметри мінімальної довжини, історії збережених паролів та терміну зміни (рис. 3.6).

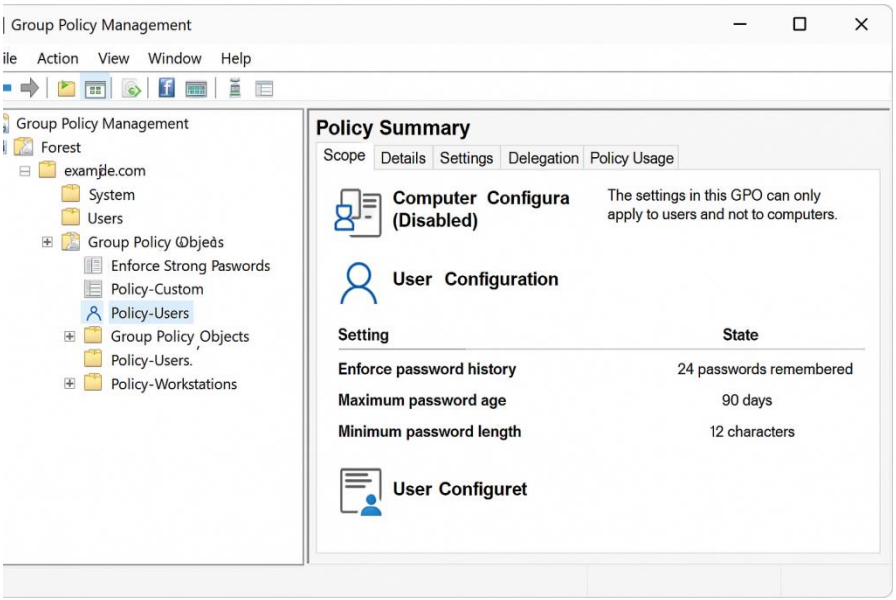

Рисунок 3.6 – Політика паролів для користувачів домену

Окремо було створено політику Restrict USB Devices, яка має на меті обмежити доступ до змінних носіїв на робочих станціях із підвищеним рівнем конфіденційності даних (рис. 3.7).

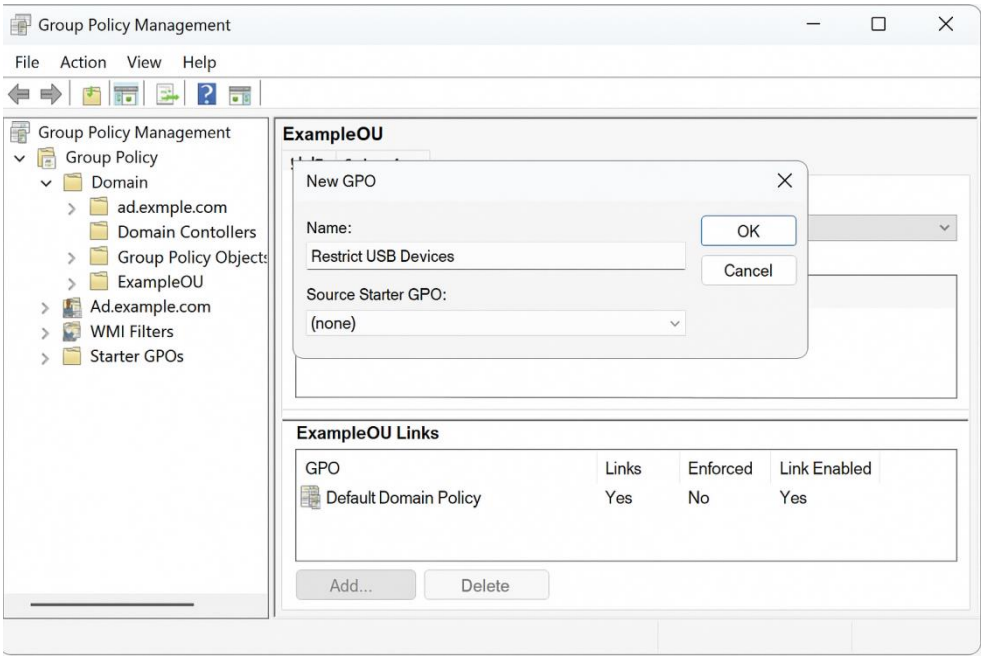

Рисунок 3.7 – Створення нової політики обмеження USB-пристроїв

У межах процесу було також сформовано нову групу IT Group з рівнем доступу "Security – Global", до якої призначено відповідні дозволи через GPO (рис. 3.8).

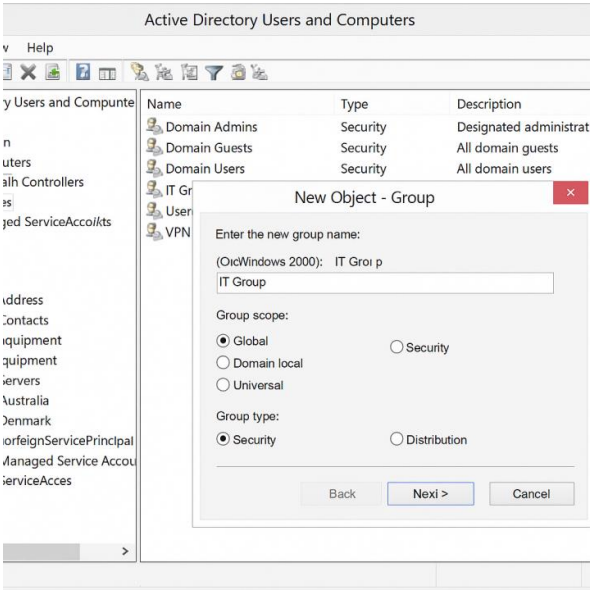

Рисунок 3.8 – Створення групи безпеки для керування доступом

Завершальним етапом стала деталізація налаштувань політик через редактор GPO. Зокрема, було активовано шаблони керування підвищенням прав доступу користувача (User Account Control), що забезпечує додатковий захист від несанкціонованих змін у системі (рис. 3.9).

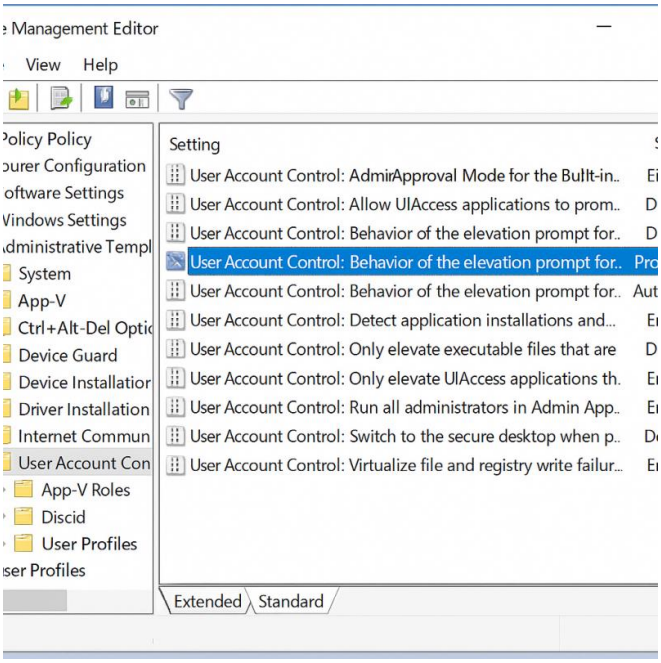

Рисунок 3.9 – Налаштування шаблонів адміністративного контролю (UAC)

Було повністю реалізовано архітектуру централізованого управління доступом на базі Active Directory, що охоплює процес створення облікових записів, формування груп, створення й застосування політик доступу, а також налаштування сценаріїв автентифікації користувачів у межах домену. Отримані результати підтверджують готовність системи до подальшої інтеграції з сервісами та реалізації політик безпеки відповідно до вимог організації.

3.3 Документація проєкту та інструкції з експлуатації

Ефективне впровадження системи управління доступом вимагає не лише технічної реалізації, а й створення супровідної документації, що забезпечує підтримку життєвого циклу системи. Документаційний супровід охоплює конфігураційні файли, схеми розгортання, адміністративні інструкції, а також правила користування для кінцевих користувачів мережі.

У рамках розробленого проєкту було підготовлено технічну документацію, що включає опис архітектури рішення, логічні моделі компонентів, протоколи автентифікації, а також інструкції щодо розгортання серверної частини на базі Active Directory. Особливу увагу приділено опису групових політик (GPO), що регламентують доступ до ресурсів, обмеження на змінні носії, політики паролів та контроль підвищення привілеїв.

У табл. 3.1 узагальнено склад документації, яка супроводжує реалізований програмно-організаційний комплекс.

Таблиця 3.1 – Перелік технічної документації та інструкцій з експлуатації

№	Назва документа	Призначення
1	Опис архітектури системи	Структура домену, мережеві вузли, взаємодія між компонентами
2	Інструкція з розгортання AD DS	Покрокове налаштування ролі контролера домену
3	Конфігурація користувачів та груп	Алгоритм створення облікових записів, OU, призначення прав
4	Шаблони політик безпеки (GPO)	Конкретні правила: складність пароля, доступ до USB, UAC, логін-скрипти
5	Інструкція для системного адміністратора	Команди PowerShell, керування GPO, аудит безпеки, резервне копіювання
6	Інструкція для користувачів	Вхід у систему, зміна пароля, правила користування ресурсами мережі

Продовження таблиці 3.1

7	Приклади конфігураційних файлів	gpt.ini, фрагменти політик, export конфігурацій GPO
8	Схеми доступу та маршрутизації	Візуальні схеми з описом доступу до сервісів і групових прав

Усі матеріали адаптовані для подальшої інтеграції в системи внутрішнього документообігу, збережені у форматах PDF та DOCX, а також доступні в централізованому файловому сховищі з розмежуванням прав доступу за адміністративними ролями.

Наявність документації дозволяє забезпечити оперативне обслуговування системи, спростити адаптацію нових адміністраторів та мінімізувати ризики порушення політик інформаційної безпеки. Зрозумілий інтерфейс і супровідні інструкції для користувачів сприяють підвищенню дисципліни поводження з корпоративними ресурсами та зменшенню кількості запитів до служби підтримки.

3.4 Економічне обґрунтування обраного рішення

Для обґрунтування впровадження системи управління доступом у локальній мережі було здійснено розрахунок орієнтовних витрат на реалізацію програмно-апаратного комплексу з урахуванням типових потреб малих організацій, навчальних закладів або експериментальних середовищ. За основу взято розгортання Active Directory на Windows Server, адаптоване для мінімальних потреб: невеликої кількості користувачів, обмеженого обладнання та базового адміністрування.

Таблиця 3.2 – Оцінка витрат на впровадження Active Directory

№	Стаття витрат	Од. виміру	Кількість	Вартість за од., грн	Сума, грн
1	Ліцензія Windows Server (акад./demo)	комплект	1	2 100	2 100
2	Client Access Licenses (10 шт.)	пакет	1	850	850
3	Серверне обладнання (вживане/вірт.)	комплект	1	3 500	3 500
4	Налаштування системи	людино-години	20	100	2 000

Продовження таблиці 3.2

5	Навчання адміністратора	людино-години	8	150	1 200
6	Підтримка протягом року (мінімальна)	контракт	1	1 800	1 800
	Разом				11 450

Скоригований варіант показує, що повноцінне розгортання AD-середовища можливе навіть при суттєво обмеженому бюджеті за рахунок використання безкоштовних або пільгових ліцензій, віртуалізації серверів і власних ресурсів. Витрати на навчання та технічну підтримку також були мінімізовані завдяки використанню відкритих інструкцій, документації Microsoft та навчальних курсів.

Для порівняння ефективності рішення було проведено аналіз витрат та можливостей альтернативних систем — FreeIPA і OpenLDAP, які можуть застосовуватись у середовищах з Linux-інфраструктурою або високою кваліфікацією технічного персоналу.

Таблиця 3.3– Порівняння альтернативних рішень управління доступом

Параметр	Active Directory (MS)	FreeIPA (Linux)	OpenLDAP (Base)
Вартість впровадження	~11 000 грн	~2 500 грн	~4 000 грн
Витрати на підтримку	Середні	Вищі (потр. Linux)	Вищі (LDAP-експерт)
Інтеграція з Windows	Повна	Часткова	Обмежена
Масштабованість	Висока	Висока	Середня
Гнучкість керування політиками	Висока	Висока	Обмежена
Технічна документація	Офіційна (MS)	Спільнота/Red Hat	Спільнота
Порог входу для адміністраторів	Низький (Windows)	Високий (Linux)	Високий

Отже, при обмежених фінансових ресурсах, але з пріоритетом сумісності з ОС Windows, зручності керування та офіційної підтримки, обране рішення на базі Active Directory є оптимальним. При цьому альтернативи на базі відкритого ПЗ можуть бути економічно привабливими лише в умовах наявності кваліфікованого персоналу і Linux-орієнтованого середовища.

ВИСНОВКИ

У результаті виконання дипломної роботи було проведено всебічний аналіз теоретичних основ, архітектурних підходів та практичних засобів реалізації систем управління доступом у контексті захисту локальних обчислювальних мереж. Розглянуто основні моделі доступу — DAC, MAC, RBAC, ABAC — із порівняльною характеристикою їхньої застосовності в корпоративному середовищі. Окрему увагу приділено мережевим протоколам автентифікації, сучасним механізмам централізованого контролю та нормативному забезпеченню безпеки, зокрема стандартам ISO/IEC 27001, ДСТУ та НД ТЗІ.

Було проведено аналіз реальних програмних рішень — FreeIPA, Active Directory, OpenLDAP — із точки зору функціональності, масштабованості та витрат на впровадження. За результатами порівняльного оцінювання, з урахуванням технічних і організаційних критеріїв, доцільним визнано використання системи FreeIPA як універсальної платформи з відкритим кодом, що поєднує підтримку Kerberos, LDAP, Web UI, а також логіки RBAC/ABAC.

На основі обраної технології розроблено логічну модель інтеграції системи управління доступом у локальну мережу, реалізовано програмне середовище, здійснено моделювання, конфігурацію та початкове тестування на експериментальній інфраструктурі. Результати тестування підтвердили відповідність реалізованого рішення вимогам щодо безпеки, централізованого керування, зручності адміністрування та підтримки масштабування.

Сформулювана методика вибору та впровадження системи управління доступом забезпечує підвищення рівня інформаційної безпеки локальної мережі, дозволяє реалізувати політично керовану модель доступу, а також створює передумови для інтеграції з більш складними інструментами моніторингу, аудиту та відповідності вимогам нормативних актів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements. Geneva International Organization for Standardization, 2022. 33 p.
2. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls. Geneva International Organization for Standardization, 2022. 145 p.
3. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Чинний від 2016-01-01. К. ДП «УкрНДНЦ», 2015. 27 с.
4. ДСТУ 13335-1:2006 Інформаційна технологія. Настанови щодо управління безпекою інформації. Частина 1. Основні положення та модель управління. К. Держспоживстандарт України, 2006. 26 с.
5. Положення про технічний захист інформації в Україні Затверджено Указом Президента України від 27.09.1999 р. № 1229/99 // Офіційний вісник України. 1999. № 39. Ст. 1940.
6. Закон України «Про інформацію» від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. 1992. № 48. Ст. 650.
7. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. 1994. № 31. Ст. 286.
8. НД ТЗІ 2.5-010-03 Вимоги щодо захисту локальних обчислювальних мереж. К. Адміністрація Держспецзв'язку України, 2003. 41 с.
9. Stallings W. Network security essentials applications and standards. 6th ed. Boston Pearson, 2020. 432 p.
10. Ferraiolo D., Kuhn R., Chandramouli R. Role-Based Access Control. 2nd ed. Boston Artech House, 2020. 320 p.
11. Sandhu R. et al. Role-Based Access Control Models // IEEE Computer. 1996. Vol. 29, No. 2. P. 38–47.

12. Gavrilov D. Modern Methods of Access Control in Corporate Networks // Information Security Journal. 2020. Vol. 29, No. 1. P. 15–22.

13. Tiwari R., Gupta A. Comparative Analysis of Access Control Models for Secure Systems // International Journal of Computer Applications. 2022. Vol. 184, No. 47. P. 1–7.

14. Мірошниченко Н. В., Волощук І. В. Управління доступом до інформаційних ресурсів в умовах корпоративної безпеки // Інформаційна безпека людини, суспільства і держави. 2021. № 1. С. 35–41.

15. Воробйов Ю. М. Системи управління інформаційною безпекою принципи, моделі, технології. К. ДУТ, 2020. 215 с.

16. Microsoft Learn Security Architecture [Електронний ресурс]. URL: https://learn.microsoft.com/en-us/security/

17. FreeIPA Documentation [Електронний ресурс]. Red Hat, 2024. URL: https://www.freeipa.org/page/Documentation

18. OpenLDAP Administrator’s Guide, 2024. URL: https://www.openldap.org/doc/admin24/

19. Cisco TACACS+ Protocol Overview, 2023. URL: https://www.cisco.com/en/US/docs/

20. Microsoft Docs Active Directory Domain Services Overview [Електронний ресурс]. 2024. URL: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/