ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система контролю доступу до корпоративної мережі на базі Keycloak»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Віталій Пивоварський
(підпис)

Виконав: здобувач вищої освіти групи БСД-44
Пивоварський Віталій
(прізвище, ім'я)

Керівник ДМІТРІЄВ В.Є
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___” _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пивоварському Віталію Ярославовичу
(прізвище, ім’я)

1. Тема кваліфікаційної роботи:
«Система контролю доступу до корпоративної мережі організації на базі Keycloak»

керівник кваліфікаційної роботи Дмітрієв В.Є.
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2024 р.

3. Вихідні дані до кваліфікаційної роботи
інформаційні ресурси організації;
рішення Red Hat Keycloak;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми контролю доступу до корпоративної мережі.
2. Аналіз методів та засобів контролю доступу до корпоративної мережі на базі Keycloak.
3. Розроблення рекомендацій щодо контролю доступу до корпоративної мережі

на базі Keycloak.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми контролю доступу до корпоративної мережі організації.	02.03.2025р.-04.05.25р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	05.03.25р.-15.03.25р.	
3.	Аналіз методів та засобів контролю доступу до корпоративної мережі організації .	17.03.25-07.04.25 р.	
4.	Практична реалізація варіанту контролю доступу до корпоративної мережі на базі Keycloak.	10.04.25р.-10.05.25р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів контролю доступу до корпоративної мережі організації.	12.05.25р.-20.05.25р.	
6.	Оформлення результатів дослідження.	21.05.25р.-31.05.25р.	
7.	Підготовка доповіді до захисту.	01.06.25р.-06.06.2025р.	

Здобувач вищої освіти _____ Віталій Пивоварський
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ В.Є.Дмітрієв
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи:38 сторінки, 10 рисунків, 12 джерел, 3 таблиці.

Об'єкт дослідження – контроль доступу до корпоративної мережі організації.

Предмет дослідження – методи та засоби контролю доступу до корпоративної мережі організації на базі Keycloak.

Мета роботи: розробити варіант системи на базі рішення Keycloak та рекомендації щодо застосування методів та засобів контролю доступу до корпоративної мережі організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння,експертна оцінка,моделювання

Системи контролю доступу до корпоративної мережі відіграють важливу роль у підвищенні безпеки корпоративної мережі організації. Контроль доступу до корпоративної мережі є критично важливим аспектом забезпечення кібербезпеки .

Система включає в себе технології, які контролюють доступ до різних ресурсів корпоративної мереж,моделюванняі, захищаючи її від несанкціонованого доступу, зловмисників та потенційних внутрішніх загроз.

В роботі досліджено проблему контролю доступу до корпоративної мережі організації, визначено його мету та завдання. Проведено аналіз існуючих методів та засобів контролю доступу до корпоративної мережі організації. Досліджено методи та засоби контролю доступу до корпоративної мережі організації на базі Keycloak. Визначено призначення, основні функції та склад системи контролю доступу .

На основі досліджень проведених в роботі запропоновано варіант системи контолю доступу до корпоративної системи організації на базі Keycloak.

Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів контролю доступу до корпоративної мережі організації.

Галузь використання – кібербезпека інформаційних систем у корпоративному середовищі.

КОРПОРАТИВНА МЕРЕЖА,КОНТРОЛЬ ДОСТУПУ,СИСТЕМА КОНТРОЛЮ,ДОСТУП ДО КОРПОРАТИВНОЇ МЕРЕЖІ,СПИСОК КОНТРОЛЮ ДОСТУПУ,КОНТРОЛЬ ДОСТУПУ НА ОСНОВІ РОЛЕЙ

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 6

ВСТУП ……..…….. 7

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ ……..… 9

1.1 Аналіз проблеми контолю доступу до корпоративної мережі ……... 9

1.2 Аналіз підходів до контолю доступу до корпоративної мережі……..... 12

1.3 Аналіз існуючих рішень з контолю доступу до корпоративної мережі … 15

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ KEYCLOAK……19

2.1 Архітектура та компоненти рішення Keycloak ……. ……...19

2.2 Призначення та основні функції компонентів Keycloak ……...22

2.3 Процеси функціонування рішення Keycloak …….23

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК ОРГАНІЗАЦІЇ …….....26

3.1 Варіант розгортання системи контролю доступу до корпоративної мережі на базі Keycloak ……..…..……26

3.2 Порядок впровадження системи контролю доступу в рішенні Keycloak……..29

3.3 Рекомендації щодо застосування методів та засобів контролю доступу до корпоративної мережі організації ……..34

ВИСНОВКИ ……..……..37

ПЕРЕЛІК ПОСИЛАНЬ 39

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 41

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD — Active Directory — служба каталогів від Microsoft
API — Application Programming Interface — програмний інтерфейс для взаємодії компонентів
CLI — Command Line Interface — інтерфейс командного рядка
DAC — Discretionary Access Control — дискреційний контроль доступу
GUI — Graphical User Interface — графічний інтерфейс користувача
HTTP / HTTPS — HyperText Transfer Protocol / Secure — протокол передавання гіпертексту (з шифруванням або без)
IAM — Identity and Access Management — управління ідентичністю та доступом
IDP — Identity Provider — постачальник ідентифікації
JWT — JSON Web Token — формат токена для передачі інформації про користувача
Keycloak — відкрита платформа управління ідентифікацією та доступом з підтримкою SSO, OAuth2, OpenID Connect, SAML
LDAP — Lightweight Directory Access Protocol — протокол доступу до служби каталогів
MAC — Mandatory Access Control — мандатний контроль доступу
MFA / 2FA — Multi-Factor Authentication / Two-Factor Authentication — багатофакторна / двофакторна автентифікація
OAuth2 — Open Authorization 2.0 — протокол авторизації
OIDC — OpenID Connect — протокол автентифікації, побудований поверх OAuth2
PBAC — Policy-Based Access Control — контроль доступу на основі політик
RB**AC** — Role-Based Access Control — контроль доступу на основі ролей
SAML — Security Assertion Markup Language — XML-базований протокол обміну даними автентифікації
SP — Service Provider — постачальник сервісу
SSO — Single Sign-On — єдиний вхід
UI — User Interface — інтерфейс користувача
UI/UX — User Interface / User Experience — інтерфейс і досвід користувача

ВСТУП

Актуальність дослідження. У сучасному цифровому середовищі корпоративні мережі є серцем інформаційної інфраструктури будь-якої організації. Саме через ці мережі передаються критично важливі дані, відбувається взаємодія між підрозділами, зберігається конфіденційна інформація та здійснюється доступ до бізнес-систем. У зв'язку з цим зростає ризик несанкціонованого доступу, витоку даних, атак з боку зовнішніх та внутрішніх зловмисників.

Особливої актуальності проблема набуває в умовах активного переходу до віддаленої роботи, використання хмарних сервісів та мобільних пристроїв. Це суттєво розширює межі корпоративної мережі, а отже — ускладнює контроль над тим, хто, коли і до чого має доступ. У таких умовах традиційні методи безпеки стають недостатніми, і зростає потреба у впровадженні сучасних моделей контролю доступу, таких як рольовий доступ (RBAC), контекстно-залежний доступ, або концепція нульової довіри (Zero Trust).

Актуальність дослідження також зумовлена зростанням вимог до інформаційної безпеки з боку міжнародних стандартів (наприклад, ISO/IEC 27001), а також законодавства про захист персональних даних (ЗУ «Про захист персональних даних»), Закону України «Про захист інформації в інформаційно-комунікаційних системах»

Таким чином, питання ефективного контролю доступу до корпоративної мережі є одним із ключових для забезпечення цілісності, конфіденційності та доступності корпоративних ресурсів, що й зумовлює актуальність обраної теми.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів контролю доступу до корпоративної мережі організації.

Об'єкт дослідження – контроль доступу до корпоративної мережі організації.

Предмет дослідження – методи та засоби контролю доступу до корпоративної мережі організації на базі Keycloak.

Мета роботи: розробити варіант системи на базі рішення Keycloak та рекомендації щодо застосування методів та засобів контролю доступу до корпоративної мережі організації.

Наукові завдання:

дослідити сутність проблеми контролю доступу до корпоративної мережі організації;

проаналізувати основні підходи до контролю доступу до корпоративної мережі організації;

проаналізувати існуючі рішення із контролю доступу до корпоративної мережі організації;

проаналізувати методи та засоби контролю доступу до корпоративної мережі організації на базі Keycloak ;

запропонувати варіант системи контролю доступу до корпоративної мережі організації на базі Keycloak;

розробити рекомендацій щодо застосування методів та засобів контролю доступу до корпоративної мережі організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння,моделювання,ризик-аналіз.

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів контролю доступу до корпоративної мережі організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ.

1.1. Аналіз проблеми контолю доступу до корпоративної мережі.

В умовах стрімкого розвитку інформаційних технологій питання захисту корпоративних інформаційних систем набуває все більшої актуальності. Одним із ключових аспектів інформаційної безпеки є контроль доступу до корпоративної мережі.

Контроль доступу до корпоративної мережі є критично важливим аспектом забезпечення кібербезпеки. Внутрішні загрози, зокрема від співробітників, можуть бути не менш небезпечними, ніж зовнішні атаки. Згідно з дослідженням, кількість кіберінцидентів, викликаних внутрішніми загрозами, зросла на 47% за останні роки

За даними Accenture, 43% атак спрямовані на малий і середній бізнес, лише 14% цих компаній готові захищатися,хоча відповідно до законодавства (стаття 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах»[2]) відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно Identity and Access Management Report від Cybersecurity Insiders [1]:

86% кіберфахівців вважають управління доступом важливою частиною своєї стратегії безпеки.Проблема з правами доступу у звіті виступає на другому місці: 70% організацій мають принаймні кількох користувачів з надмірними правами доступу. 66% вважають RBAC(рольову модель доступу**)** найважливішою для управління доступом. 49% організацій планують інвестувати в багатофакторну автентифікацію та управління привілейованим доступом у наступні 12 місяців.

Про важливість цієї проблеми свідчать дані з Identity and Access Management Report[1],згідно яким витрати на IAM-рішення очікується понад $25 млрд до 2026р. (рис.1.1.1).

Рис.1.1.1.Темпи зростання витрат на IAM-платформи

Доступ до внутрішніх інформаційних ресурсів повинен бути чітко регламентований, аби уникнути витоку конфіденційних даних, несанкціонованого втручання та порушення цілісності інформації.

На сьогоднішній день корпоративні мережі охоплюють багато філій по всій Україні та об'єднують тисячі співробітників. Це створює складне середовище, в якому контроль доступу повинен не лише захищати систему, а й забезпечувати зручність та ефективність щоденної роботи персоналу. У зв’язку з цим виникає ряд проблем:

велика кількість користувачів та ролей, що вимагає складної системи розмежування доступу;

підключення зовнішніх постачальників та партнерів, що ускладнює управління привілеями;

гібридна інфраструктура (поєднання локальних та хмарних сервісів), що створює додаткові вектори атаки;

потреба в мобільному доступі (віддалена робота), яка часто супроводжується використанням незахищених каналів зв'язку.

Також актуальною проблемою є застарілість або фрагментованість рішень для контролю доступу. Часто у великих організаціях, різні відділи можуть використовувати різні механізми автентифікації, що ускладнює централізо-ваний контроль і моніторинг.

Крім того, загрози з боку соціальної інженерії, фішингу, компрометації облікових записів вимагають не лише технічних рішень, але й впровадження політик безпеки, навчання персоналу та регулярного аудиту системи доступу.

Таким чином, ефективний контроль доступу до корпоративної мережі є критичним елементом загальної системи кібербезпеки, і вимагає комплексного підходу, який буде розглянуто у наступних розділах.

Узагальнення найважливіших проблеми системи контролю доступу можна побачити в таблиці 1.1.1

Таблиця 1.1.1

Проблеми контролю доступу в інформаційних системах

№	Проблема	Опис	Джерело інформації
1	Надмірні привілеї користувачів	Користувачі отримують більше прав, ніж потрібно, що створює ризики витоку або зловживання	NIST SP 800-12 Rev. 1
2	Відсутність принципу найменших привілеїв	Система не обмежує доступ до мінімально необхідного рівня	NIST SP 800-53
3	Недостатнє журналювання доступу	Відсутність або неповне логування ускладнює аудит та виявлення порушень	ISO/IEC 27001:2022
4	Недійсні або застарілі облікові записи	Старі облікові записи (напр. звільнених працівників) не деактивуються	OWASP Access Control Cheat Sheet
5	Обхід механізмів контролю доступу	Вразливості дозволяють отримати доступ, минаючи контрольні механізми	OWASP Top 10 (Broken Access Control)

№	Проблема	Опис	Джерело інформації
6	Недостатня сегментація ролей	Ролі не розмежовані, що призводить до конфліктів інтересів та зловживань	NIST Role-Based Access Control (RBAC)
7	Ручне управління правами доступу	Відсутність автоматизації спричиняє помилки при наданні або відкликанні прав	SANS Institute Security Policy Templates
8	Відсутність регулярного перегляду прав	Немає перевірки актуальності наданих прав користувачам	CIS Controls v8 (Control 6: Access Control Management)

1.2. Аналіз підходів до контролю доступу до корпоративної мережі

Контроль доступу — це процес обмеження доступу користувачів до ресурсів інформаційної системи відповідно до їхніх повноважень. Ефективна реалізація цього процесу потребує вибору відповідної моделі контролю доступу та засобів її впровадження.

Серед основних підходів до контролю доступу вирізняють:

1. Рольовий контроль доступу (RBAC — Role-Based Access Control)

Цей підхід передбачає призначення користувачам певних ролей**,** які, у свою чергу, мають визначені права доступу до ресурсів. RBAC є одним з найбільш поширених методів у корпоративному середовищі через свою гнучкість та масштабованість. Він дозволяє централізовано керувати привілеями, що зменшує ризик людської помилки та полегшує аудит.

2. Дискреційний контроль доступу (DAC — Discretionary Access Control)

DAC надає власнику ресурсу право визначати, хто може мати доступ до нього. Це більш гнучкий, але менш безпечний підхід, оскільки користувачі можуть передавати доступ іншим без додаткових перевірок. У великих організаціях DAC може бути джерелом вразливостей через відсутність централізованого контролю.

3. Мандатний контроль доступу (MAC — Mandatory Access Control)

MAC базується на політиках безпеки, які встановлюються централізовано і не можуть змінюватись користувачами. Кожен об'єкт і суб'єкт має свій рівень секретності, і доступ дозволяється лише при відповідності рівнів. Цей підхід часто використовується у державних структурах, але також може бути ефективним у банківській сфері для захисту особливо критичної інформації.

4. Контроль доступу на основі політик (PBAC — Policy-Based Access Control)

Цей сучасний підхід враховує не тільки ролі чи рівні секретності, а й динамічні умови — час, місцезнаходження, пристрій, контекст запиту. Наприклад, якщо співробітник намагається увійти в систему з-за меж України або поза робочим часом, доступ може бути обмежено. PBAC ідеально підходить для гібридних та хмарних середовищ, де ризики вищі.

5. Zero Trust (Нульова довіра)

Цей підхід ґрунтується на принципі "нікому не довіряти за замовчуванням". Кожен запит до ресурсу перевіряється незалежно від його походження — навіть якщо користувач знаходиться всередині корпоративної мережі. Zero Trust вимагає постійної автентифікації, авторизації та моніторингу. У контексті,наприклад, банківської сфери, цей підхід має високий потенціал завдяки здатності протистояти як зовнішнім, так і внутрішнім загрозам.

6. *IAM-платформи (Identity and Access Management)*

Окремою групою виділяється цей сучасний підхід,що набирає все більшої популярності . Це комплексні рішення, що реалізують вищезазначені моделі у вигляді програмних систем.Прикладами найбільш відомих рішень є Microsoft Entra ID (колишній Azure AD), Okta, OneLogin, Keycloak.Серед переваг цих засобів відзначається єдина точка аутентифікації (SSO),мультифакторна

аутентифікація (MFA),Управління життєвим циклом користувачів,Аудит і журналювання доступу.

Узагальнюючи, вибір конкретного підходу до контролю доступу залежить від багатьох факторів(таблиця 1.2.1): масштабу організації, характеру даних, рівня загроз, технічної інфраструктури. Найчастіше застосовується комбінований підхід**,** який поєднує кілька моделей для досягнення оптимального балансу між безпекою та ефективністю роботи персоналу.

Таблиця 1.2.1

Порівняльна таблиця основних підходів до контролю доступу:

Модель	**Гнучкість**	**Безпека**	**Складність впровадження**	**Рекомендовано для**
RBAC	Середня	Середня	Низька	Невеликі та середні компанії
ABAC	Висока	Висока	Висока	Великі компанії, державні установи
PBAC	Висока	Висока	Середня	Хмарні системи, критичні сервіси
DAC	Висока	Низька	Низька	Тимчасові проєкти, стартапи
MAC	Низька	Висока	Висока	Армія, держсектор, банки
IAM	Залежить від платформи	Висока	Середня	Будь-які організації

1.3. Аналіз існуючих рішень з контролю доступу до корпоративної мережі організації.

Сучасні рішення з контролю доступу реалізують різні моделі доступу: від рольового (RBAC) до атрибутивного (ABAC) та Zero Trust.
Вибір залежить від масштабу організації,типу інфраструктури (локальна чи хмарна),бюджету,потреб в інтеграції.

Віртуальні приватні мережі (VPN) – це найстаріші та найбільш поширені варіанти для забезпечення безпечного віддаленого доступу до корпоративних ресурсів організації. VPN створює зашифрований звязок між пристроєм користувача та корпоративною мережею,і при цьому забезпечує конфіденційність даних при передачі через публічні або ненадійні мережі(наприклад , Інтернет). До переваг VPN відноситься ,звичайно,простота реалізації з використанням уже існуючої мережевої інфраструктури.Зараз майже всі операційні системи мають вбудовану підтримку VPN-клієнтів.Звичайно ,через тривалий термін використання ці технології вже перевірені часом.

Існує кілька типів VPN.Вирізняють тип,що забезпечує доступ віддалених співробітників до корпоративних ресурсів через спеціальні клієнтські застосунки (Remote Access VPN).Інша група – це з’єднання різних філій організації в єдину віртуальну мережу (Site-to-Site VPN). SSL VPN забезпечує доступ через веб-браузер. Через виклики сьогодення VPN уже не завжди відповідає стандартам кібербезпеки через обмежений контроль,низьку гнучкість та проблеми з мобільністю. Хоча VPN залишається актуальним способом віддаленого підключення, він дедалі більше поступається новітнім моделям доступу, таким як ZTNA , IAM.

Окремою групою можна виділити системи контролю доступу до мережі NAC. Ця група рішень контролю доступу дозволяє перевіряти стан пристрою перед наданням доступу до мережі. Сюди відносяться всім відомі антивіруси,

оновлення, сертифікати. Перевагами цього підходу можна назвати контроль на рівні мережі та вчасне виявлення та ізоляція підозрілих пристроїв. Прикладом можуть служити рішення Cisco Identity Services Engine (ISE) та Aruba ClearPass

Новим і сучасним підходом до рішення контролю доступу вважається ZTNA , що базується на принципі "нікому не довіряй, перевіряй завжди". Доступ надається тільки після автентифікації користувача та перевірки стану пристрою, навіть якщо він знаходиться всередині корпоративної мережі. Гнучкий доступ до ресурсів незалежно від розташування, при цьому зведення до мінімуму ризиків горизонтального переміщення у разі компрометації виділяють його сере інших рішень.Також цей підхід краще відповідає сучасній архітектурі хмарних сервісів.

Системи управління ідентичністю та доступом (IAM) теж є сучасним рішенням контролю доступу до корпоративної системи організації.Вони забезпечують централізоване керування користувачами, автентифікацією, авторизацією та аудитом.Системи дозволяють ефективно контролювати, хто і до яких ресурсів має доступ.

Розглянуто найпоширеніші рішення, що реалізують ефективну систему контролю доступу , яка дозволяє гарантувати, що тільки авторизовані користувачі можуть отримати доступ до певних ресурсів відповідно до своєї ролі або рівня прав: як відкриті, так і комерційні системи, що використовуються в корпоративному середовищі(таблиця 1.3.1).

1. Microsoft Active Directory (AD).

Це централізована служба каталогів, розроблена компанією Microsoft, яка є основою систем управління користувачами у Windows-орієнтованих середовищах**.** Active Directory забезпечує**:**

централізоване зберігання інформації про користувачів, пристрої та ресурси; єдину точку автентифікації; політики безпеки та контролю доступу через Group Policy Objects (GPO)**;** підтримку SSO у рамках домену.

Цьому рішенню зазвичай надають перевагу через глибоку інтеграцію з Windows-сервісами,високу стабільність і масштабованість,широку підтримку інструментів аудиту та моніторингу.

Водночас висока вартість ліцензування,складність розгортання в гетерогенному (різнорідному) середовищі,залежність від Microsoft-інфраструктури стають недоліками для впровадження AD в організаціях.

2. LDAP-рішення (OpenLDAP, Apache Directory)

LDAP (Lightweight Directory Access Protocol)- це відкритий протокол для доступу до розподілених служб каталогів. Найпопулярніші реалізації: OpenLDAP та Apache Directory Server.

Відкритий код, безкоштовна ліцензія,підтримка масштабування,можливість кастомізації структури каталогів відносять до переваг цього вибору.

Але відсутність сучасного інтерфейсу для керування,складна конфігурація для новачків,відсутність вбудованих механізмів авторизації ,що потребує інтеграції з іншими системами ставить під сумнів правильність вибору цього рішення.LDAP часто використовується в якості джерела ідентичностей, а не повноцінної IAM-системи.

3. Хмарні комерційні платформи (Okta, Auth0, OneLogin)

Ці рішення є сервісами ідентифікації як послуги (IDaaS). Вони дозволяють швидко інтегрувати контроль доступу без значних витрат на інфраструктуру.

Okta підтримує OpenID Connect, OAuth2, SAML 2.0.,Дає змогу налаштовувати MFA, SSO, lifecycle management,Має готові інтеграції з великою кількістю хмарних застосунків (Google Workspace, Salesforce, Zoom тощо).

Auth0 орієнтований на розробників,можлива швидка інтеграція з веб- і мобільними застосунками,є можливість кастомізації UI входу.

OneLogin включає Підтримку SCIM, SAML, OAuth2. Сервіс орієнтований на корпоративні середовища з високими вимогами до безпеки. Можливе швидке розгортання,його інтерфейс з мінімальними технічними бар'єрами,підтримує готові шаблони доступу та політик. Але залежить від сторонніх сервісів,необхідна щомісячна плата за користувача та є обмеження у безкоштовних тарифах.

Таблиця(рис. 1.3.1),згенерована ШІ [5],коротко і наочно ілюструє основні підходи до контролю доступу.

Таблиця 1.3.1.

Порівняльний аналіз рішень з контролю доступу до корпоративної мережі

№	Рішення	Тип доступу	Основні переваги	Основні недоліки
1	IAM-платформи (Okta, Keycloak, Azure AD)	Централізований (SSO, MFA)	Єдина точка входу, масштабованість, аудит	Складність налаштування, залежність від хмари
2	VPN (OpenVPN, Cisco AnyConnect)	Мережевий доступ	Шифрування трафіку, простота впровадження	Відсутність контролю на рівні ресурсів, ризики компрометації
3	NAC (Cisco ISE, Aruba ClearPass)	Доступ на рівні мережі	Перевірка стану пристрою, ізоляція підозрілих	Висока вартість, складність інтеграції
4	ZTNA (Zscaler, Cloudflare Access)	Контекстний доступ	Zero Trust, гнучкість, детальний контроль	Вимагає перебудови архітектури, вартість

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ KEYCLOAK.

2.1 Архітектура та компоненти рішення Keycloak

Переглянувши ряд рішень,зроблено висновок,що одним із найефективніших підходів до реалізації безпечного та гнучкого управління доступом є

використання систем централізованої автентифікації, таких як Keycloak [4]. Це open-source рішення, яке надає інструменти для управління користувачами, ролями, сесіями, дозволами та інтеграції з іншими сервісами.

На цей час Keycloak обирають компанії-гіганти – лідери галузі: Amazon, Netflix, Salesforce, JPMorgan Chase; LinkedIn, Twitter, eBay [12].

Keycloak - це відкрита платформа управління ідентичностями та доступом (IAM), розроблена компанією Red Hat. Вона дозволяє централізовано реалізовувати: автентифікацію та авторизацію; єдиний вхід (SSO) між декількома системами; підтримку стандартів: OAuth2, OpenID Connect, SAML 2.0; інтеграцію з LDAP, Active Directory, Google, GitHub тощо; багатофакторну автентифікацію (2FA/MFA); гнучке керування ролями, групами та політиками доступу.

Також Keycloak підтримує розгортання у Docker та Kubernetes, що дозволяє легко масштабувати систему.

Це повністю безкоштовний з відкритим вихідним кодом продукт,що має потужний веб-інтерфейс адміністратора,велика спільноту користувачів та документацію,можливість розширюватись через розробку власних розширень. .

Разом з тим у Keycloak відносно складна первинна конфігурація,інтерфейс може змінюватися у нових версіях, що потребує адаптації,потрібен окремий сервер для хостингу (на відміну від IDaaS-рішень).

Keycloak побудований за модульною архітектурою, що забезпечує масштабованість і розширюваність системи. Його основні компоненти дозволяють централізовано керувати користувачами, ролями та процесами автентифікації. Платформа підтримує сучасні протоколи безпеки — OAuth 2.0, OpenID Connect, SAML 2.0 — що дозволяє легко інтегрувати її з внутрішніми системами організації.

Основні компоненти:

1. Realm (реалм) — логічно ізольована область у межах сервера Keycloak. У межах одного реалму адміністратор керує користувачами, клієнтами, групами, ролями та політиками. Наприклад, для різних департаментів компанії можна створити окремі реалми.
2. Users (користувачі) — облікові записи співробітників або сервісів. Кожен користувач має унікальне ім’я, пароль, ролі, а також атрибути (наприклад, email, підрозділ).
3. Groups (групи) — логічні об’єднання користувачів для централізованого управління доступом. Наприклад, група "HR-відділ" може мати набір типових ролей.
4. Roles (ролі) — визначають права доступу користувачів. Можуть бути двох типів: Realm-level roles та Client-level .
5. Clients (клієнти) — застосунки, які взаємодіють з Keycloak (вебсайти, API, мобільні додатки). Клієнти можуть автентифікувати користувачів та отримувати інформацію про них.
6. Authentication Flows — сценарії автентифікації, які визначають послідовність перевірок при вході в систему (наприклад, логін → пароль → двофакторна перевірка).
7. Identity Providers (IdP) — зовнішні постачальники автентифікації, такі як Google, Facebook, GitHub, LDAP, Active Directory. Користувачі можуть входити через зовнішні облікові записи.
8. Admin Console — веб-інтерфейс для адміністраторів, що дозволяє налаштовувати всі компоненти системи.
9. Account Console — особистий кабінет користувача, де він може змінити пароль, переглянути активні сесії та налаштувати 2FA.

2.2. Призначення та основні функції компонентів Keycloak

Кожен із компонентів Keycloak має своє чітке функціональне призначення, яке дозволяє реалізувати ефективну систему контролю доступу.

Компонент	Функції
Realm	Ізоляція даних користувачів, клієнтів та ролей; незалежне адміністрування
User	Зберігання даних про користувача; автентифікація та атрибути
Group	Групування користувачів; призначення загальних ролей
Role	Визначення прав доступу; забезпечення авторизації
Client	Інтерфейс взаємодії з додатками; надання токенів
Authentication Flow	Гнучке налаштування сценаріїв автентифікації
Identity Provider	Автентифікація через сторонні сервіси (LDAP, SAML, Google)
Token (JWT)	Перенесення інформації про користувача між Keycloak і клієнтом
Admin Console	Повне адміністрування конфігурації реалмів і користувачів
Account Console	Особисте керування доступом користувачем

Завдяки цій структурі Keycloak дозволяє швидко масштабувати систему, обслуговувати багато організацій (multi-tenancy) та забезпечувати безперервність бізнес-процесів.

2.3. Процеси функціонування рішення Keycloak

Платформа Keycloak як система контролю доступу ефективно забезпечує три ключові властивості безпеки: конфіденційність, цілісність та доступність. Конфіденційністьу Keycloak досягається завдяки таким функціям як Аутентифікації користувачів, Контролю доступу на основі ролей (RBAC), Використанню захищених протоколів.

Цілісність забезпечується цифровим підписування токенів, автоматичною ротацією ключів підпису, журналюванням змін і подій, підтримкою конфігураційних резервних копій.

Доступність у Keycloak реалізовано можливістю розгортання в кластерному режимі, Docker-контейнерами та підтримкою Kubernetes, Health-чеками та сервісами готовності.

У роботі Keycloak основну роль відіграє процес автентифікації та авторизації. Взаємодія клієнта з Keycloak здійснюється за кількома стандартними етапами.

Типовий процес автентифікації:

1. Користувач намагається отримати доступ до ресурсу (вебзастосунку, API).
2. Його перенаправляє на сторінку входу Keycloak.
3. Користувач вводить облікові дані, проходить двофакторну перевірку (якщо налаштовано).
4. Keycloak перевіряє дані й створює токен доступу (Access Token), ID Token та Refresh Token.
5. Клієнт отримує токен і надає користувачу доступ згідно з його ролями.
6. Користувач може переглядати або змінювати налаштування профілю через Account Console.
7. Адміністратор може моніторити сесії, блокувати доступ або змінювати політики через Admin Console.

Додаткові функціональні можливості:

Single Sign-On (SSO) — користувач входить один раз і отримує доступ до всіх підключених систем.

Аудит і логування — всі дії записуються для контролю та безпеки.

Інтеграція з DevOps — Keycloak легко впроваджується через Docker, Kubernetes або Helm-чарти.

Гнучке управління політиками доступу — на основі атрибутів користувача, IP-адреси, часу доби тощо.

2.3.1.Як працює визначення ролей та доступів у Keycloak:

Keycloak підтримує два основних типи ролей:

Realm roles	Глобальні ролі, що діють у межах всього realm'a (області Keycloak). Можуть бути призначені напряму користувачам або групам.
Client roles	Ролі, специфічні для конкретного клієнта (наприклад, вебзастосунку або API). Дають доступ лише в межах відповідного клієнта.

Ролі можна призначати напряму користувачам або призначати групам, а користувач отримує ролі автоматично, якщо входить у цю групу.
Також можна видавати через зовнішні провайдери (наприклад, LDAP або зовнішній IDP).
Групи в Keycloak — це спосіб логічно об’єднати користувачів. Тут можна: створити групу; призначити їй одну або кілька ролей; додати до неї користувачів. Це дозволяє масштабовано керувати доступом.

2.3.2. Як вибирається модель доступу у Keycloak:

У Keycloak є кілька моделей контролю доступу, і вибір тієї чи іншої залежить від складності системи**,** рівня безпеки**,** який потрібно забезпечити, а також типу клієнтів (веб, мобільний, API).

RBAC (Role-Based)-основна модель у Keycloak**.**Тут визначаються realm roles або client roles**;**призначаються ролі через GUI або API;на стороні клієнта (застосунку) перевіряється наявність потрібної ролі в токені.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАСТОСУВАННЯ МЕТОДІВ ТА ЗАСОБІВ КОНТРОЛЮ ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1. Варіант розгортання системи контролю доступу до корпоративної мережі на базі Keycloak.

Для зручності в користуванні та для спрощення встановлення взято контейнерний варіант встановлення за допомогою Docker [6].

Процес встановлення та налаштування складається з наступних кроків:

1. З офіційного сайту встановлено Docker Desktop:

https://www.docker.com/products/docker-desktop

Для цього спочатку завантажено інсталятор .exe. Потім запущено завантажений інсталятор, під час встановлення залишено опцію ‘WSL 2 backend’ увімкненою.

Необхідно перевірити, що Docker працює.
Для цього запущено Docker Desktop і через 10–20 секунд отримано повідомлення “Docker is running”.В командному рядку Windows введено:

docker version,

щоб побачити версію програми та впевнитися,що сервіс працює(рис.3.1.1.1).

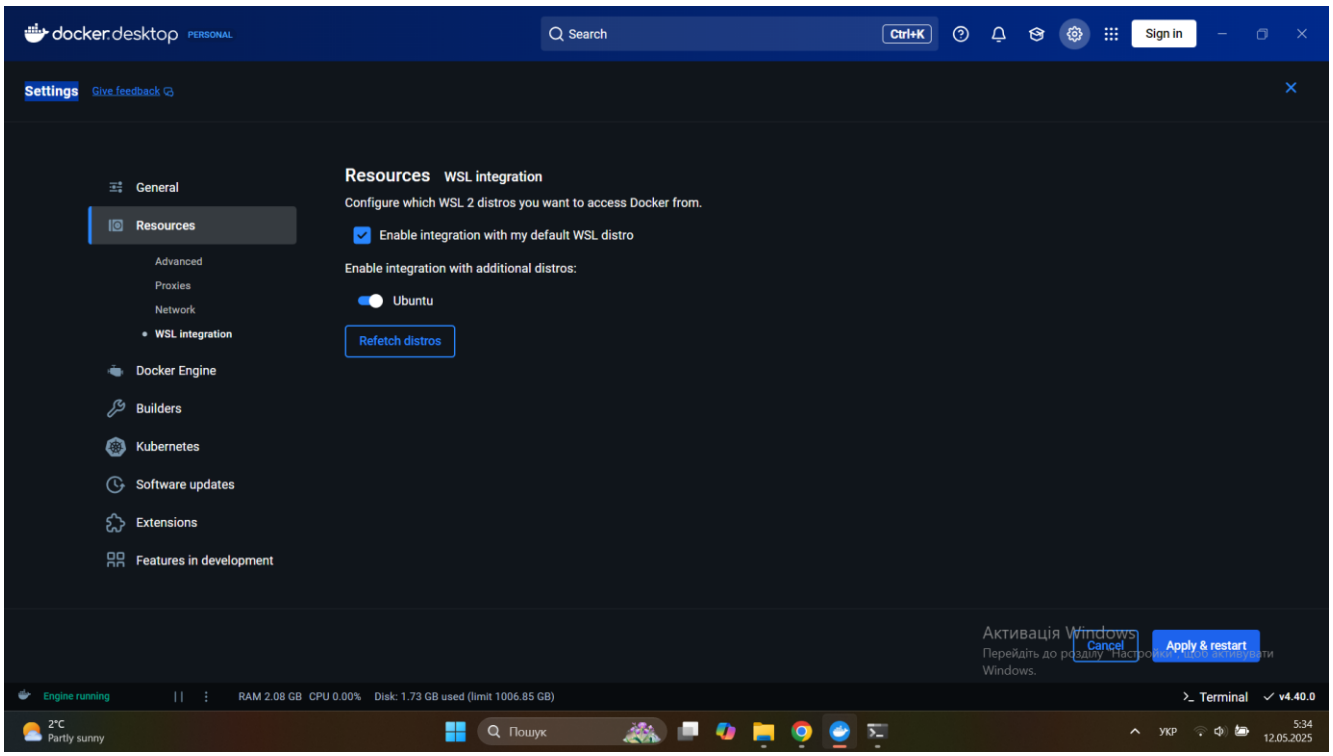

Рис.3.1.1.1. Вікно налаштувань Docker Desktop

В налаштуваннях встановлено ‘WSL integration’ та підключено Ubuntu.

1. Слідуючим кроком в середовищі Ubuntu введено команди для загрузки контейнера Keycloak в Docker.Основними вимогами для встановлення Keycloak є встановлений Docker та вільний порт 8080.

Для відкриття Keycloak в Docker набрано слідуючі команди (рис.3.1.2.1):

```
docker run -p 8080:8080 \
  -e KEYCLOAK_ADMIN=admin \
  -e KEYCLOAK_ADMIN_PASSWORD=admin \
  quay.io/keycloak/keycloak:24.0.1 \
  start-dev
```

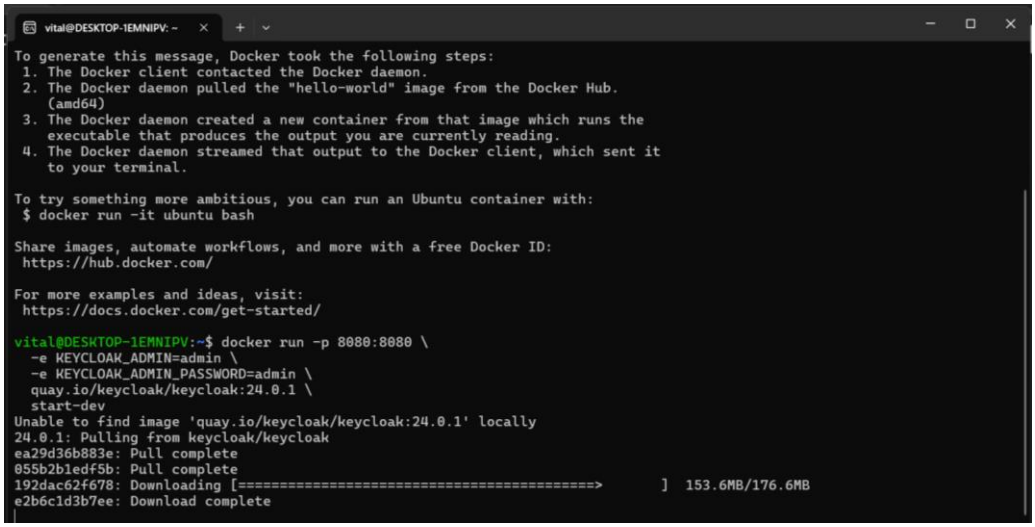

Рис.3.1.2.1. Приклад відкриття Keycloak в Docker

Тут виконано слідуючі кроки :

- відкрто порт 8080 (локально);
- створено адміністратора з логіном admin і паролем admin ;

- завантажено офіційний образ Keycloak із Red Hat репозиторію (quay.io);
- запущено його в режимі розробника.

Перед встановленням Keycloak в середовищі Docker необхідно переконатися,що на комп'ютері є встановлена потрібна операційна система.В нашому випадку це буде Ubuntu,оскільки це одна з найпоширеніших платформ,яка забезпечує стабільну роботу Docker та має зручне середовище для управління контейнерами (рис.3.1.2.2).

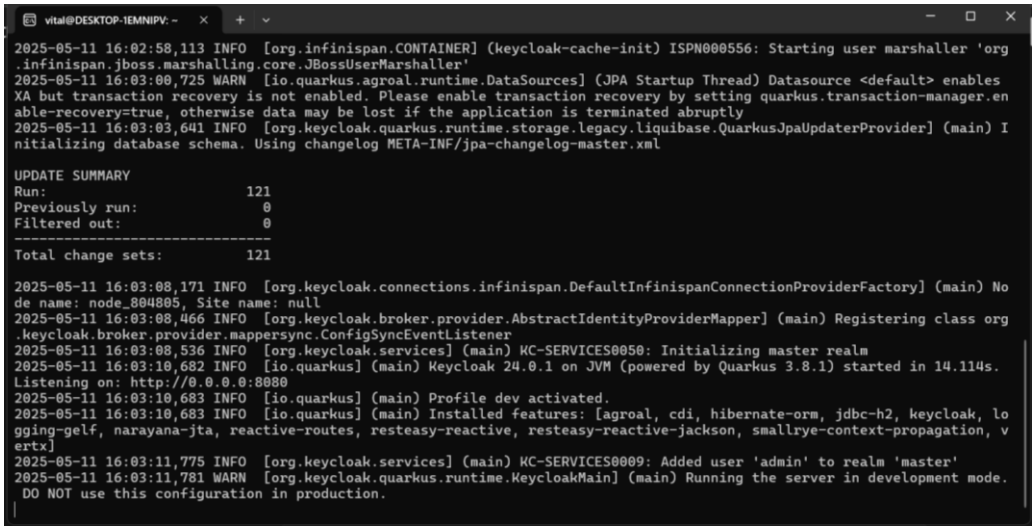

Рис.3.1.2.2.Установка Ubuntu

3.Після запуску Keycloak в середовищі Docker здійснено доступ до нього в браузері Windows на сторінку,яку створено раніше(рис.3.1.3.1):

http: // localhost:8080

Порт 8080 використовується тут тому,що Keycloak ,запущений у Docker,приймає запити на порті 8080.

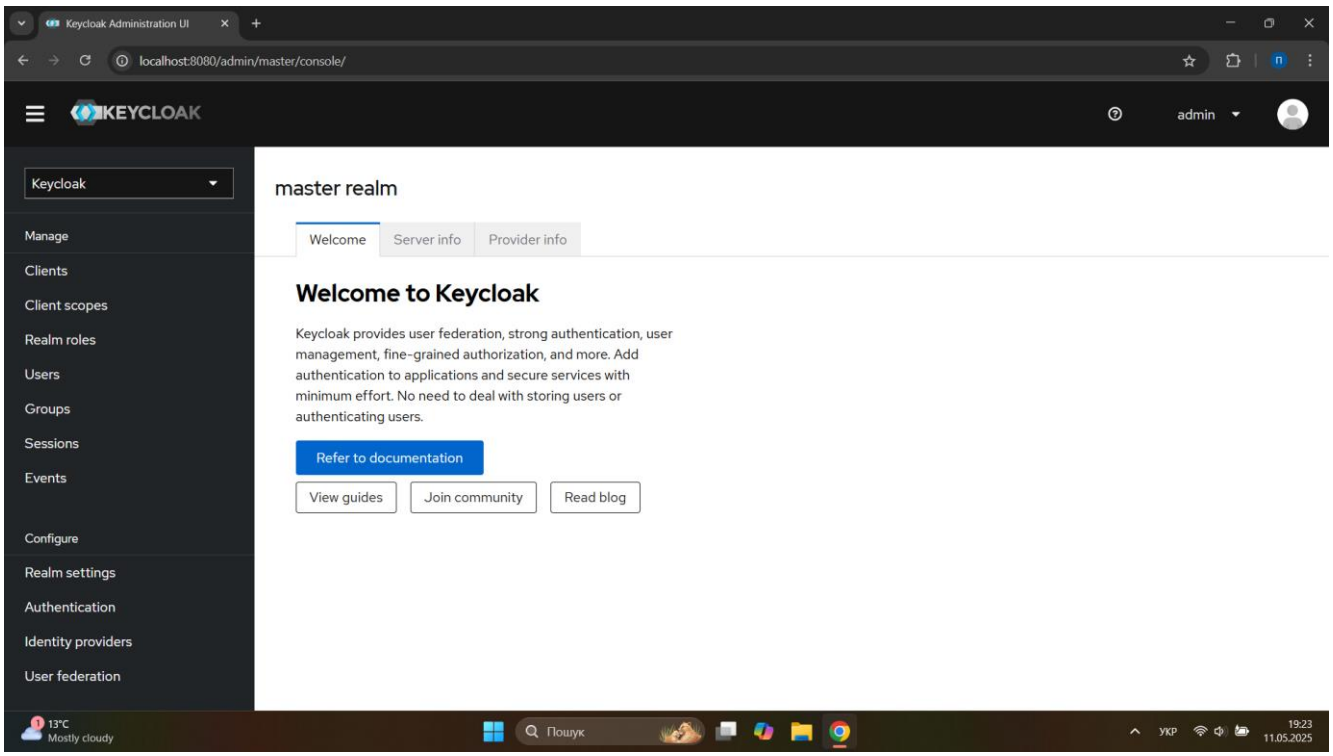

Рис.3.1.3.1. Сторінка входу в Keycloak

3.2. Порядок впровадження системи контролю доступу в рішенні Keycloak.

Впровадження системи контролю доступу на базі Keycloak передбачає послідовне налаштування компонентів системи управління ідентичністю та доступом.Після інсталяції Keycloak обов’язково створюється адміністративний обліковий запис,щоб керувати сервісом та налаштовувати параметри безпеки.

Створення домену (realm) є обов’язковим наступним кроком,оскільки це буде основою, в межах якої створюються всі інші елементи: налаштування клієнтів, ролей і користувачів, а також інтеграцію з внутрішніми або зовнішніми сервісами. Кожен етап (рис.3.2.1) потребує уваги до безпеки, цілісності та зручності керування правами доступу.

Термін	Пояснення
Realm	Ізольована зона керування користувачами та налаштуваннями безпеки
Client	Застосунок, який використовує Keycloak для автентифікації

Термін	Пояснення
User	Користувач системи
Role	Роль (напр. "admin", "employee") — визначає права доступу
Group	Група користувачів
Protocol	OAuth2, OpenID Connect, SAML

Рис.3.2.1 Таблиця термінів Keycloak

Налаштування компонентів системи:

3.2.1. У Keycloak реалм — це ізольоване середовище з власними користувачами, ролями, клієнтами та політиками безпеки. Кожна організація або окремий проєкт може мати свій реалм для кращого розділення доступу. Створення реалму — перший крок під час налаштування системи, що дозволяє адміністратору визначити загальні параметри доступу, автентифікації та інтеграції. Кожен реалм функціонує незалежно, що підвищує масштабованість та безпечність архітектури Keycloak.

Створено власний realm — окрему область для користувачів, ролей, додатків.

Для цього вибрано функцію ‘Create realm",заповнено поля та підтверджено Create(рис.3.2.1.1).

Здійснено вхід в створений реалм(рис.3.2.1.2)

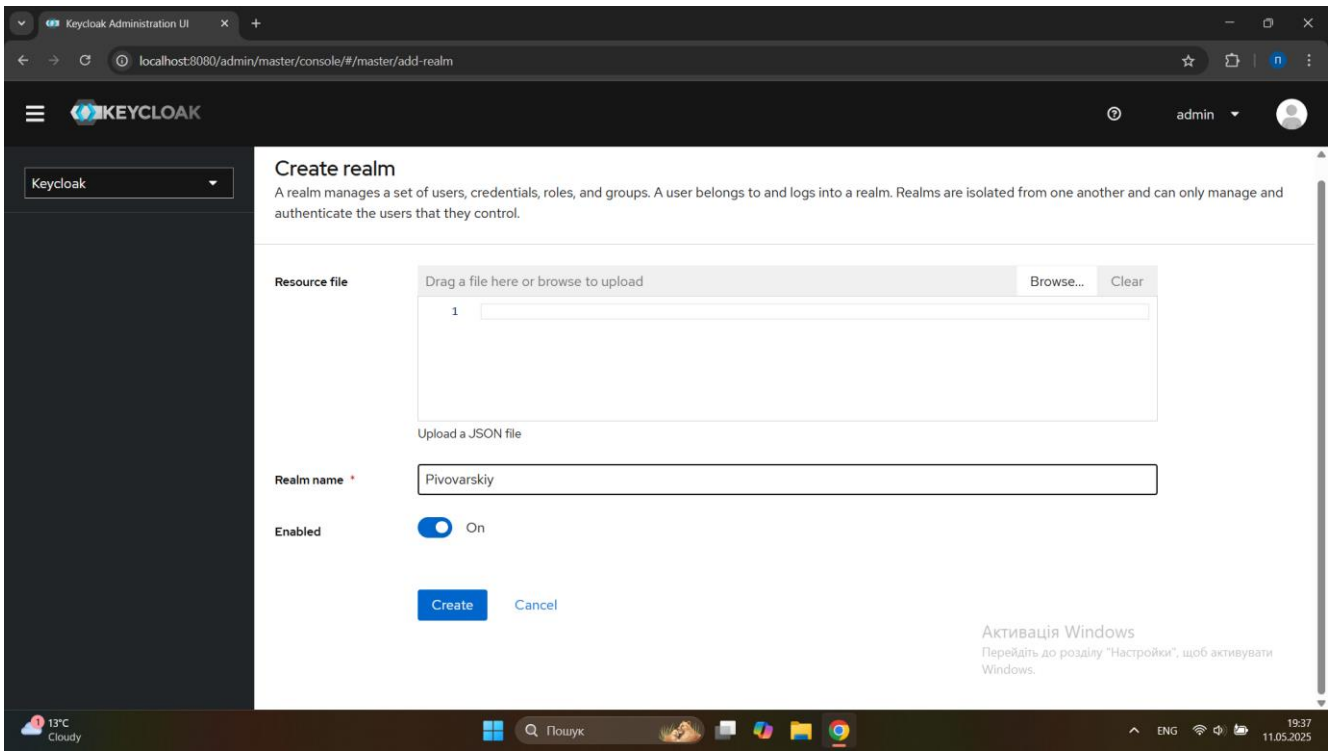

Рис 3.2.1.1. Створення реалму Pivovarskiy

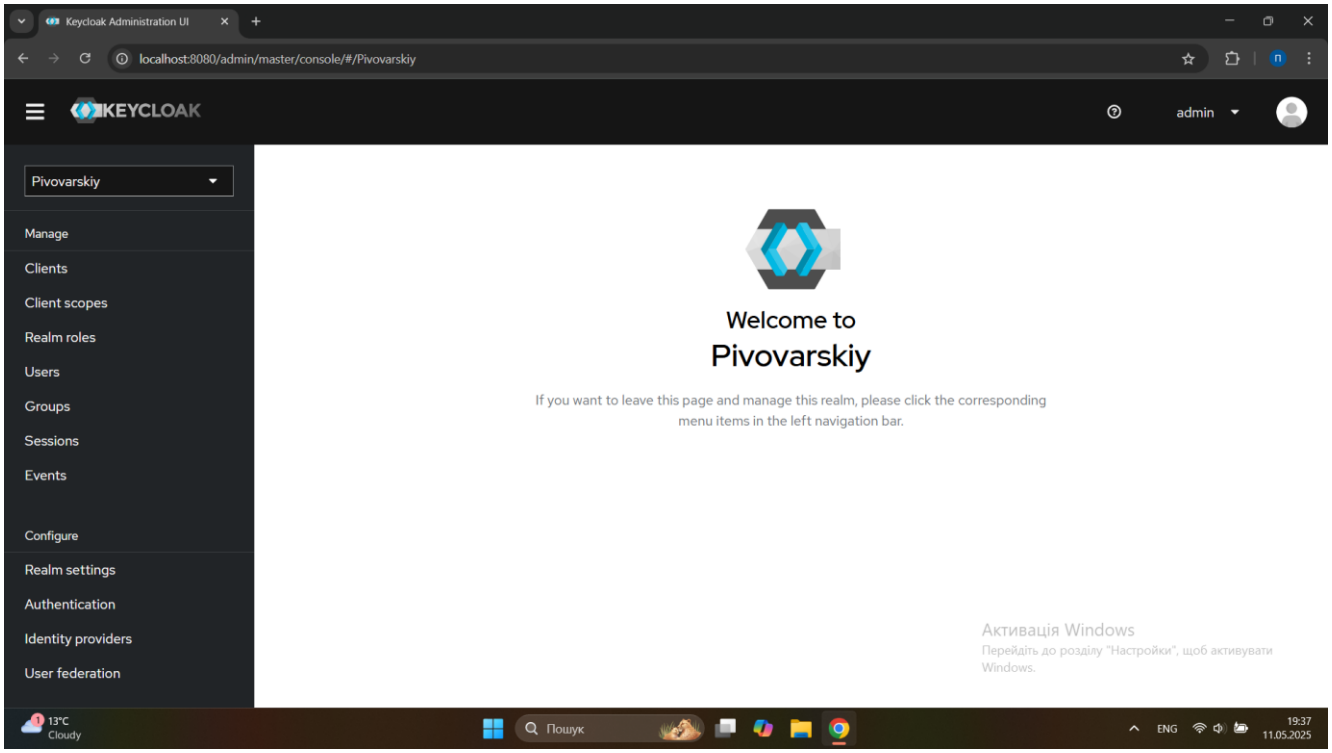

Рис.3.2.1.2 Вхід в створений реалм

3.2.1. В реалмі Pivovarskiy створено користувачів emp1,mgr1,admin1(рис.3.2.2.1)**.**

В нашому прикладі створено облікові записи користувачів вручну.Але Keycloak дозволяє адміністраторам створювати облікові записи користувачів вручну або автоматизовано. Для кожного користувача вказується ім’я, email, ім’я користувача (username), статус облікового запису та, за потреби, пароль. Додатково можна налаштувати атрибути, рольову модель та методи автентифікації (наприклад, MFA). Після створення користувача адміністратор може одразу призначити йому ролі або включити до певних груп. Це забезпечує централізоване управління ідентичностями та контроль доступу до корпоративних ресурсів.

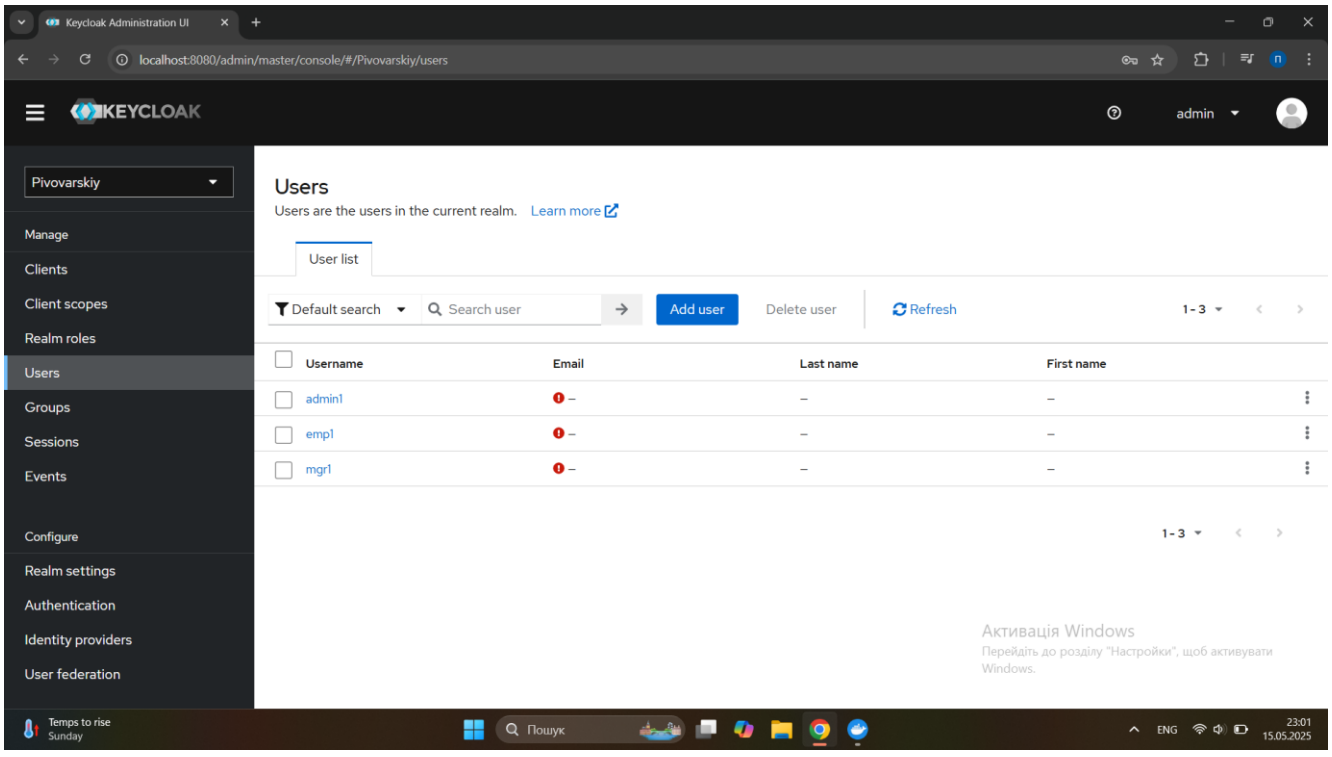

Рис.3.2.2.1. Створення користувачів в реалмі Pivovarskiy

3.2.3. Створено ролі(права доступу) manager,admin,employee(рис.3.2.3.1)

Під час створення ролі використано уже саму назву для визначення рівнів доступу користувачів до ресурсів. Також вказано її назву, опис та, за потреби, зв'язок її з іншими ролями.

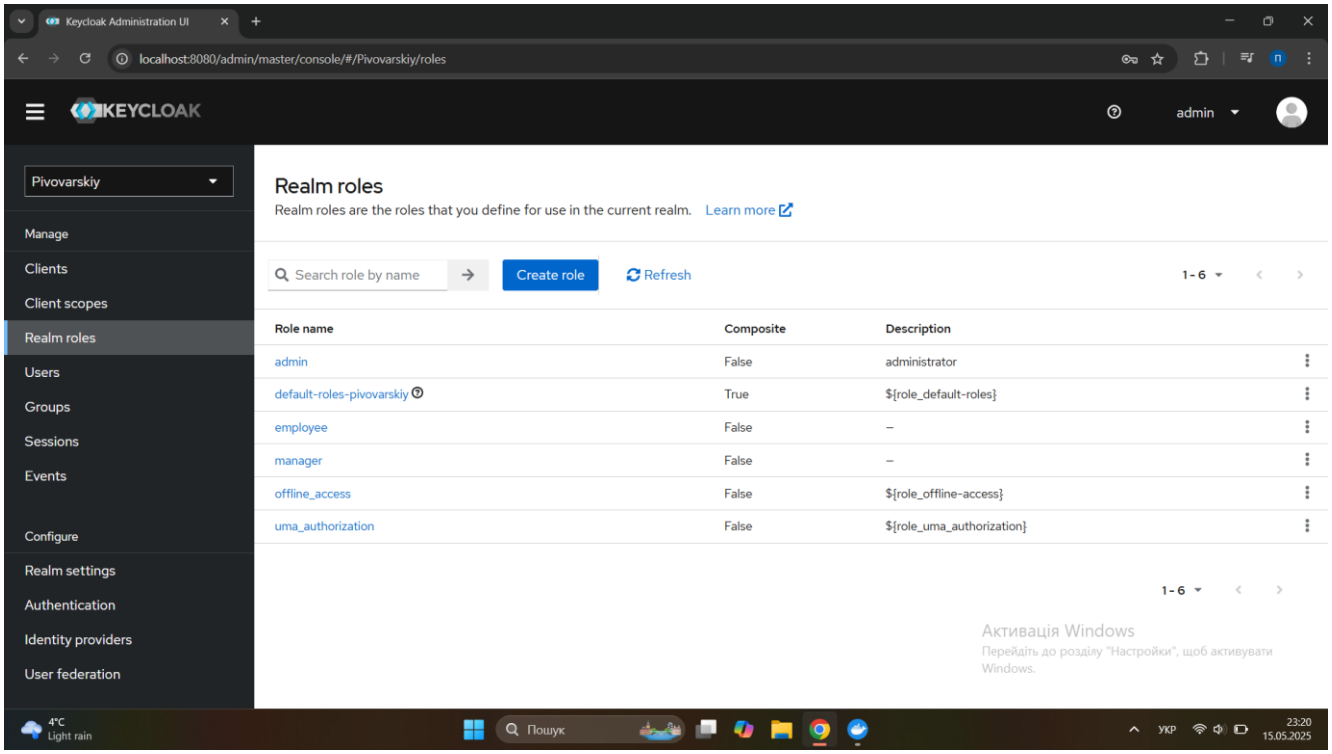

Рис.3.2.3.1. Створення ролей admin,manager

3.2.4. У Keycloak клієнт - це додаток або сервіс, який потребує автентифікації користувачів через систему управління доступом. Під час створення клієнта адміністратор вказує його ідентифікатор, тип доступу (наприклад, публічний чи конфіденційний), URL-адреси перенаправлення після входу, а також налаштування авторизації та протоколу (наприклад, OpenID Connect або SAML). Клієнти є ключовим елементом інтеграції Keycloak із корпоративними вебсайтами, мобільними додатками чи API. Правильне налаштування клієнта забезпечує контроль доступу, безпечну авторизацію та централізоване керування сесіями користувачів.

Створено та налаштовано Client stud_vit (Рис.3.2.4.1).

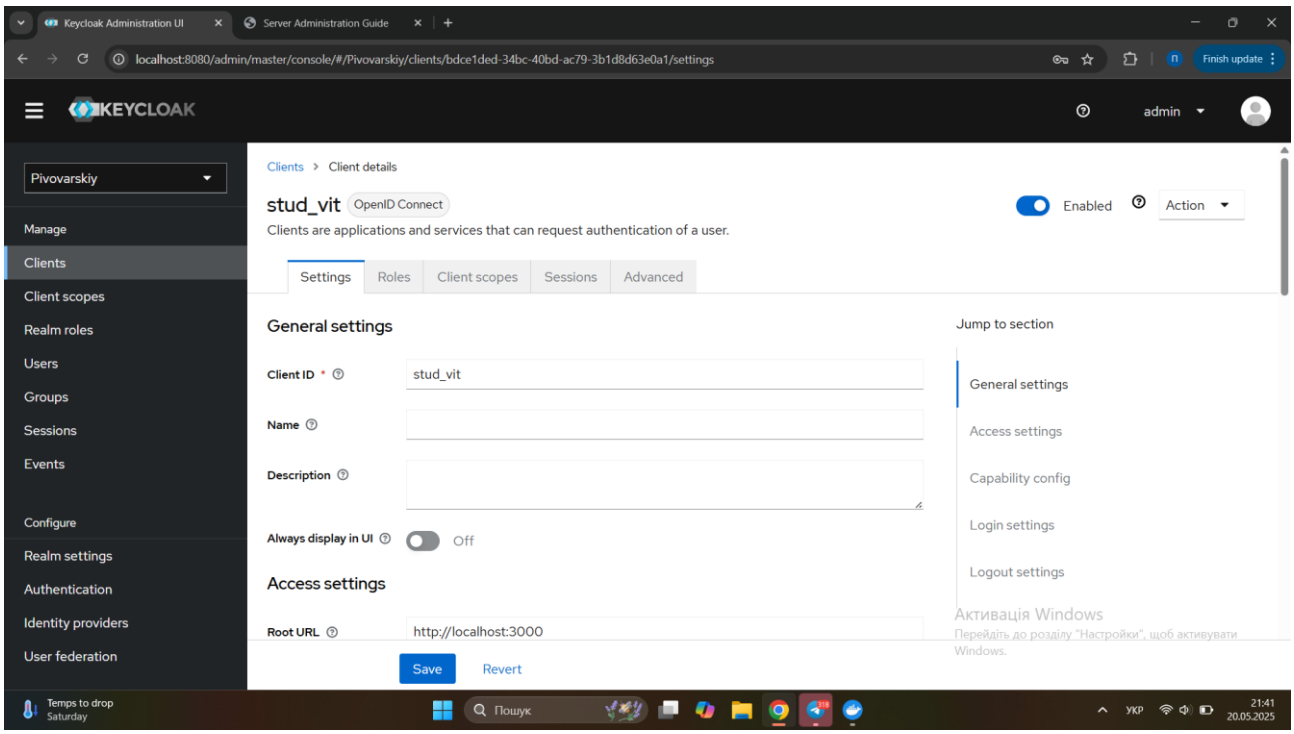

Рис.3.2.4.1. Створеннння Client stud_vit

3.3. Рекомендації щодо застосування методів та засобів контролю доступу до корпоративної мережі організації

З метою забезпечення ефективного, безпечного та масштабованого контролю доступу до корпоративної мережі, доцільно реалізувати комбінацію сучасних методів автентифікації, авторизації та моніторингу доступу з використанням платформи Keycloak**.**

Рекомендовано впроваджувати слідуючі засоби:

Використовувати Keycloak як єдиний центр автентифікації .Це дозволить об’єднати доступ до всіх внутрішніх сервісів і застосунків за принципом Single Sign-On (SSO). Таке об’єднання підвищить зручність для користувачів, а також спростить адміністрування.

Необхідно активувати MFA ,щоб зменшити ризики компрометації облікових записів.Зробити це можна, наприклад, через OTP (одноразові паролі), мобільні додатки (Google Authenticator, FreeOTP) або FIDO2-ключі.

Реалізувати модель доступу на основі ролей. У Keycloak,як ми бачили вище, можна створити ролі, які будуть призначатися користувачам або групам відповідно до їхніх посад, відділів чи рівня доступу до ресурсів.

Використовуючи API в межах корпоративної мережі, необхідно захищати їх через протоколи OAuth 2.0 або OpenID Connect з токенами, що видаються Keycloak. Це дозволяє контролювати доступ на рівні сервісів і клієнтських застосунків.

Якщо необхідно запровадити контроль сесій та моніторинг активності , Keycloak надає засоби керування активними сесіями, що дає змогу вручну завершити підозрілі або неактивні сесії. Також слід налаштувати аудит і журналювання подій входу/виходу користувачів для виявлення аномальної поведінки.

Необхідно регулярно переглядати надані ролі, доступи та неактивні облікові записи, щоб уникнути надмірних прав і потенційних векторів атак. Використовуючи сучасну IAM-систему, якою вважається Keycloak, важливо реалізовувати мережеву сегментацію (через VLAN, ACL, ZTNA-підходи) та обмежувати доступ до ресурсів лише тим, кому він справді потрібен.

Офіційні кейс-стаді, опубліковані на сайті Keycloak[4], повідомляють про використання цієї платформи компаніями Hitachi та OpenTalk. Зокрема, Hitachi впровадила Keycloak для забезпечення безпеки API в фінансовому секторі, а OpenTalk використовує його для автентифікації користувачів у своєму відеоконференц-застосунку.

Також необхідно зазначити, що Keycloak є популярним рішенням з відкритим кодом для управління ідентичністю та доступом, яке активно використовується в різних організаціях по всьому світу. Однак конкретні приклади використання в компаніях-гігантах можуть бути недоступні через політику конфіденційності або відсутність публічних заяв.

Разом з тим українська IT-компанія AgriChain агропромислового холдингу ’Астарта-Київ’ повідомила, що прийняла рішення впровадити продукт Keycloak з максимальними характеристиками безпеки, зручності та надійності.

На питання: «Чому саме Keycloak ?» ,- в компанії відповіли,що вже сьогодні користувачі IT-рішення моніторингу та управління посівами AgriChain Scout після авторизації у вікні Keycloak вільно допускаються без додаткових автентифікації до роботи з IT-рішенням з управління логістикою ТМЦ AgriChain Logistics, адже адміністратор системи Keycloak прописав відповідні ролі на доступ.

В компанії наголосили на значних перевагах цього рішення,адже до роботи з Keycloak, треба було прийти в додаток з логіном та паролем, отримувати постійний токен і далі користувача по ньому авторизувало, якщо час життя токену закінчився, починалися проблеми. Але в Oauth2 запропонували варіант з токенами, що динамічно змінюються, що зменшило можливість прямих атак, а ключі, за якими користувач авторизується на сайті, автоматично оновлюються кожні кілька хвилин. І це не єдина перевага технології. Під час вибору «єдиного вікна авторизації» фахівці AgriChain виділили три фундаментальні переваги продукту:

відкрите програмне забезпечення;

простота використання та налаштування,наявність деталізованої документації;

безпека на рівні Enterprise, що означає, що можна бути впевненими в безпеці своїх даних та додатків.Адже Keycloak використовує протоколи безпеки, такі як OAuth 2.0, OpenID Connect та SAML 2.0, які забезпечують безпеку проєкту на високому рівні, що для розробників AgriChain є дуже актуальним питанням. В компанії переконані,що впроваджують найкращі світові напрацювання,яким є рішення Keycloak[12].

Висновки

В роботі проведено дослідження проблеми контролю доступу до корпоративної мережі організації, визначено його мету та завдання. Сьогодні існують серйозні проблеми контролю доступу до корпоративної мережі організацій, оскільки щодня виникають нові і все більш витончені загрози. Спостерігається зростання ризиків для безпеки корпоративної мережі організацій, які посилюються недостатньою підготовленістю їх до протидії новим загрозам за допомогою існуючих платформ контролю доступу.

Проведено аналіз існуючих методів та засобів контролю доступу. Розглянуті рішення демонструють широкий спектр можливостей у сфері контролю доступу до корпоративних ресурсів.

Сучасні системи контролю доступу до корпоративної мережі повинні бути багаторівневими та контекстно-залежними. Відхід від традиційного VPN до IAM, ZTNA, NAC та CASB-рішень дозволяє забезпечити більш гнучке, масштабоване та безпечне середовище доступу до ресурсів організації. Оптимальне рішення часто базується на комбінуванні кількох технологій у рамках єдиної стратегії Zero Trust. Розглянуті рішення демонструють широкий спектр можливостей у сфері контролю доступу до корпоративних ресурсів. Для потреб середнього корпоративного середовища Keycloak є оптимальним вибором завдяки відкритості та безкоштовності; гнучкій системі ролей і політик; широкій підтримці сучасних стандартів безпеки; активній спільноті.

Keycloak як сучасна IAM-платформа реалізує принципи інформаційної безпеки за моделлю CIA-тріади. Завдяки цьому вона підходить для використання як у малих організаціях, так і у великих корпоративних мережах, де критично важлива безпека автентифікації та доступу до цифрових ресурсів.

Keycloak може допомогти організаціям скористатися останніми рекомендаціями, забезпечуючи комплексну систему контролю, автоматизуючи процеси реагування на інциденти та спрощуючи впровадження найкращих практик контролю доступу.

Таким чином, правильна реалізація системи Access Control організації має сприяти ефективному захисту корпоративних інформаційних ресурсів у цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Identity and Access Management Report" від Cybersecurity Ventures URL: https://cybersecurityventures.com/identity-and-access-management- report (дата звернення 25.05.25).

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах»

3. Кібербезпека України (CERT-UA) URL: https://cert.gov.ua — Національний центр кіберзахисту (дата звернення 21.05.25).

4. Keycloak Documentation

URL: https://www.keycloak.org/documentation

https://www.keycloak.org/getting-started/getting-started-docker

https://www.keycloak.org/guides (дата звернення 15.05.25р).

5. [Електронний ресурс]. OpenAI ChatGPT. URL:

https://chat.openai.com (дата звернення: 01.06.2025).

6. Docker Documentation
URL: https://docs.docker.com

(дата звернення 29.04.25).

7. Пономарьов О. А., "Засоби контролю доступу в інформаційних системах"

8. NIST Special Publication 800-162: "Guide to Attribute Based Access Control (ABAC)"
https://csrc.nist.gov/publications/detail/sp/800-162/final

9. Fortinet White Paper: "What is Zero Trust Access?"
https://www.fortinet.com/resources.

10..«Інформаційні системи та мережі» Вісника Національного університету «Львівська політехніка» URL:
https://ena.lpnu.ua/collections/f160dfed-3c17-435d-b74b-b8a85ecc9819
(дата звернення: 12.05.2025р.)

11.Аналітичний дайджест «Кібербезпека» №10/2023,Інститут проблем інформаційної безпеки НАН України.
URL: (https://ippi.org.ua) (дата звернення: 20.05.2025р.)

12. [Електронний ресурс] Чому AgriChain впроваджує продукт Keycloak? URL: https://agrichain.com.ua/chomu-agrichain-vprovadzhuye-produkt-keycloak/?utm_source=chatgpt.com