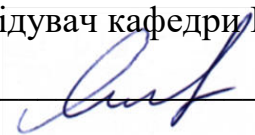


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут комп'ютерних наук та управління проєктами
Кафедра інформаційних управляючих систем та технологій

"Допущений до захисту"

Завідувач кафедри ІУСТ



к.т.н, доц. Михелєв І.Л.

" ____ " _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти "Магістр"

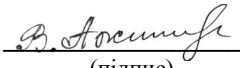
на тему: **«ДОСЛІДЖЕННЯ МЕТОДІВ СИСТЕМИ ДИНАМІЧНОГО
ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ
ПІДПРИЄМСТВА»**

Виконав: студент групи

 Качурка Д.І.
(підпис)

Керівник роботи:

К.Т.Н., ДОЦЕНТ
(посада, науковий ступінь вчене звання)

 Ажищев В.Ф.
(підпис)

м. Миколаїв – 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут комп'ютерних наук та управління проєктами
Кафедра інформаційних управляючих систем та технологій
Спеціальність 122 "Комп'ютерні науки"
Освітня програма "Комп'ютерні науки"

"ЗАТВЕРДЖУЮ"

Гарант освітньої програми

В. Ажищев

к.т.н, доц. Ажищев В.Ф.

" ____ " _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття ступеня вищої освіти "Магістр"

Студенту Качурці Даніїлу Ігоревичу

(прізвище, ім'я, по батькові)

1. Тема роботи: Дослідження методів системи динамічного призначення ролей у системах керування доступом підприємства

Керівник роботи к.т.н., доцент Ажищев В.Ф.

Затверджені наказом ректора № 1355 -уч від "14" листопада 2025 року.

2. Термін подання роботи: 15 грудня 2025 р.

3. Вихідні дані до проєкту (роботи) ДСТУ щодо обробки інформації, літературні джерела, технічна документація на існуючі аналоги систем,

4. Перелік питань, що належать до розробки (найменування розділів) Вступ. 1. Аналіз предметної області, розробка концепції на основі методів динамічного призначення ролей у системах керування доступом підприємства. 2. Розробка проєктних рішень динамічного призначення ролей у системах керування доступом підприємства. 3. Реалізація методів динамічного призначення ролей у системах керування доступом підприємства. 4. Розрахунок економічної ефективності впровадження методів динамічного призначення ролей у системах керування доступом підприємства 5. Охорона праці та техніка безпеки. 6. Охорона навколишнього середовища. Висновки. Додатки.

5. Перелік презентаційних матеріалів Діаграма варіантів використання методів динамічного призначення ролей у системах керування доступом підприємства. Діаграма декомпозиції кожного із варіантів використання методів динамічного призначення ролей у системах керування доступом підприємства. Діаграма діяльності. Концептуальна модель бази даних. Логічна модель бази даних. Фізична модель бази даних динамічного призначення ролей у системах керування доступом підприємства.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Ажищев В.Ф.	05.09.2024	22.12.2024
2	Ажищев В.Ф.	23.12.2024	15.06.2025
3	Ажищев В.Ф.	15.06.2025	25.09.2025
4	Ажищев В.Ф.	25.09.2025	14.11.2025
5	Ажищев В.Ф.	25.09.2025	14.11.2025
6	Ажищев В.Ф.	25.09.2025	14.11.2025

7. Дата видачі завдання 05 вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

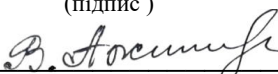
№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів роботи	Примітка
1	Аналіз предметної галузі	22.12.2024	
2	Постановка задачі	15.03.2025	
3	Розробка концепції	15.06.2025	
4	Розробка проєкту ІС	25.09.2025	
5	Реалізація проєкту	14.11.2025	
6	Розробка питань з охорони праці	14.11.2025	
7	Розробка графічних матеріалів	14.11.2025	
8	Подання роботи на перевірку на плагіат	16.11.2025	
9	Подання роботи рецензенту	20.11.2025	
10	Подання роботи на захист	15.12.2025	

Студент


(підпис)

Качурка Д.І
(ПІБ)

Керівник роботи


(підпис)

Ажищев В.Ф
(ПІБ)

Анотація

У роботі представлено дослідження методів динамічного призначення ролей у системах керування доступом підприємства. Проведено аналіз традиційних моделей контролю доступу — дискреційної DAC, мандатної MAC, рольової RBAC та атрибутно-орієнтованої ABAC. Визначено недоліки статичних підходів та обґрунтовано необхідність застосування динамічних моделей, що враховують контекст взаємодії користувача, рівень ризику та політику безпеки підприємства.

Запропоновано архітектуру системи керування доступом із динамічним призначенням ролей, реалізовану з використанням алгоритмів машинного навчання для прогнозування поведінкових патернів користувачів. Очікуваним результатом є підвищення гнучкості, адаптивності та рівня захисту корпоративних інформаційних ресурсів.

Ключові слова: керування доступом, динамічне призначення ролей, інформаційна безпека, RBAC, ABAC, машинне навчання, політика безпеки.

Abstract

The study presents research on dynamic role assignment methods in enterprise access control systems. The analysis covers traditional access control models — discretionary DAC, mandatory MAC, role-based RBAC, and attribute-based ABAC. The limitations of static approaches are identified, and the necessity of applying dynamic models that consider user interaction context, risk levels, and enterprise security policies is substantiated.

An access control architecture with dynamic role assignment is proposed, implemented using machine learning algorithms to predict user behavioral patterns. The expected outcome is increased flexibility, adaptability, and security of corporate information systems.

Keywords: access control, dynamic role assignment, information security, RBAC, ABAC, machine learning, security policy.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ДИНАМІЧНОГО ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ ПІДПРИЄМСТВА	8
1.1. Теоретичні основи систем керування доступом. Поняття та сутність систем керування доступом	8
1.2. Класифікація моделей керування доступом	8
1.3. Аналіз дискреційної та мандатної моделей керування доступом.....	9
1.3.1. Дискреційна модель (DAC)	9
1.3.2. Мандатна модель MAC	9
1.3.3 Аналіз рольової моделі керування доступом RBAC	10
1.3.4. Аналіз атрибутно-орієнтованої моделі керування доступом ABAC.....	10
1.4 Сутність динамічного призначення ролей у системах керування доступом	10
1.5. Огляд сучасних методів динамічного призначення ролей	11
1.6. Використання машинного навчання в динамічному призначенні ролей.....	12
1.7 Постановка задачі дослідження.....	13
Висновки до розділу 1	14
РОЗДІЛ 2. Проектування ІС ДИНАМІЧНОГО ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ ПІДПРИЄМСТВА	15
2.1 Концепція системи	15
2.3 Архітектура системи.....	19
2.3 Загально системні рішення	22
2.4 Статична сруктура системи	24
2.5 Діаграма послідовності.....	28
2.6 Проектування бази даних системи	29
Висновки до розділу 2	36
РОЗДІЛ 3. РОЗРОБКА ІС ПРИЗНАЧЕННЯ РОЛЕЙ	38
3.1 Фізичне розгортання системи.....	38
3.2 Вимоги до апаратного забезпечення для розробки системи	40
3.3 Вимоги до програмного забезпечення.....	41
Висновки до розділу 3	43

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ РОЗРОБКИ.....	45
4.1 Обґрунтування технічної необхідності.....	45
4.2 Розрахунок витрат на розробку системи	45
4.2.1 Витрати на оплату праці розробників.....	45
4.2.2 Витрати на інфраструктуру та середовище розробки	46
4.2.3 Загальна собівартість розробки	46
4.3 Економічна ефективність впровадження.....	46
4.3.1 Прямі економічні вигоди.....	46
4.3.2 Непрямі вигоди.....	46
4.4 Розрахунок окупності	47
Висновки з техніко-економічного обґрунтування.....	47
РОЗДІЛ 5 ОХОРОНА ПРАЦІ	48
5.1. Значення охорони праці в діяльності фахівця з інформаційних технологій	48
5.2. Аналіз небезпечних і шкідливих факторів на робочому місці.....	48
5.3. Вимоги до організації робочого місця розробника	48
5.4. Електробезпека при роботі з комп'ютерним обладнанням	49
5.5. Пожежна безпека у приміщенні розробників	49
5.6. Вимоги безпеки під час роботи з даними та інформаційними ресурсами	50
5.7. Заходи з охорони праці під час розробки програмного забезпечення ..	50
Висновки до розділу	50
РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА	51
6.1. Екологічні аспекти використання комп'ютерної техніки	51
6.2. Оптимізація енергоспоживання та ресурсів.....	51
6.3. Управління електронними відходами.....	52
6.4. Вплив інформаційної системи на екологічну політику підприємства ..	52
6.5. Дотримання екологічних стандартів та нормативів.....	53
Висновки до розділу 6	53
ВИСНОВКИ.....	54
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	56
ДОДАТОК А - Технічне завдання.....	57

ДОДАТОК Б - Інструкція користувача.....	61
ДОДАТОК В - Екранні форми розробки	64

ВСТУП

Сучасні підприємства функціонують у складному інформаційному середовищі, де безпека даних є одним із ключових чинників стабільної діяльності та конкурентоспроможності. Зі зростанням обсягів оброблюваної інформації, впровадженням хмарних технологій, розподілених обчислень і віддаленого доступу постає необхідність ефективного управління правами користувачів. Одним із найпоширеніших підходів у цій сфері є рольове керування доступом (RBAC — Role-Based Access Control), яке забезпечує розмежування доступу до ресурсів на основі ролей, визначених для певних категорій користувачів.

Однак традиційні статичні моделі RBAC не завжди відповідають вимогам сучасних динамічних підприємств, де ролі співробітників можуть змінюватися залежно від контексту діяльності, робочих процесів або середовища виконання. Тому актуальним є дослідження методів динамічного призначення ролей, які дозволяють адаптивно змінювати політику доступу в реальному часі, враховуючи ситуаційні фактори, поведінкові характеристики користувачів та ризик-орієнтовані показники.

Метою даної роботи є аналіз, порівняння та розроблення методів динамічного призначення ролей у системах керування доступом підприємства з урахуванням контекстної інформації, що забезпечує підвищення рівня інформаційної безпеки та гнучкості системи.

Для досягнення мети передбачено розв'язання таких завдань.

1. Провести системний аналіз існуючих моделей керування доступом і виявити їхні переваги та обмеження.
2. Дослідити підходи до динамічного формування ролей і контекстно-залежного керування доступом.
3. Розробити методiku динамічного призначення ролей із використанням аналітичних і машинних методів оцінювання ризиків;

4. Створити модель інформаційної системи керування доступом підприємства з підтримкою динамічного призначення ролей.

5. Провести експериментальну перевірку ефективності запропонованої методики.

Об'єктом дослідження є процес керування доступом до інформаційних ресурсів підприємства.

Предметом дослідження є методи динамічного призначення ролей у системах керування доступом.

Наукова новизна роботи полягає у розробленні адаптивної моделі призначення ролей, що враховує контекстні зміни у поведінці користувачів і дозволяє оперативно реагувати на потенційні ризики безпеки.

Практичне значення одержаних результатів полягає у можливості використання розробленої методики в інформаційних системах підприємств різного профілю для підвищення ефективності управління доступом і забезпечення цілісності корпоративних даних.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ДИНАМІЧНОГО ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ ПІДПРИЄМСТВА

1.1. Теоретичні основи систем керування доступом. Поняття та сутність систем керування доступом

Система керування доступом (СКД) — це сукупність програмних, апаратних та організаційних засобів, що забезпечують авторизацію, автентифікацію та контроль дій користувачів у межах інформаційних ресурсів підприємства. Основною метою СКД є гарантування того, що доступ до даних отримують лише ті суб'єкти, яким це дозволено відповідно до політики безпеки організації.

В основі будь-якої моделі контролю доступу лежать такі поняття *суб'єкт* — користувач, процес або система, яка ініціює запит доступу. *Об'єкт* — ресурс, до якого здійснюється доступ (файл, база даних, сервіс). *Право доступу* — тип операції, яку суб'єкт може виконувати над об'єктом читання, запис, виконання. Політика безпеки — набір правил, що визначає, за яких умов доступ є дозволеним або забороненим.

З розвитком цифрової трансформації підприємств і розширенням мережевих інфраструктур зросла складність управління правами доступу, що зумовило потребу у створенні динамічних, контекстно-залежних систем керування доступом, здатних адаптуватися до поточної ситуації без втручання адміністратора [1].

1.2. Класифікація моделей керування доступом

Моделі контролю доступу класифікуються за способом визначення та призначення прав доступу. Основними типами є дискреційна модель (DAC, Discretionary Access Control) — власник об'єкта самостійно визначає, хто може отримати доступ до його ресурсів.

Мандатна модель MAC, Mandatory Access Control — доступ визначається централізовано на основі рівнів секретності та політики безпеки.

Рольова модель RBAC, Role-Based Access Control — права доступу визначаються через ролі, які прив'язуються до посадових обов'язків користувачів.

Атрибутно-орієнтована модель ABAC, Attribute-Based Access Control — рішення про доступ приймається на основі множини атрибутів користувача, ресурсу та середовища.

Також виділяють контекстно-залежні Context-Aware Access Control та ризик-орієнтовані моделі, що є еволюційним продовженням RBAC та ABAC і використовуються в сучасних адаптивних системах.

1.3. Аналіз дискреційної та мандатної моделей керування доступом

1.3.1. Дискреційна модель (DAC)

У моделі DAC власник ресурсу має повний контроль над наданням прав доступу іншим користувачам. Дана модель реалізується за допомогою таблиць доступу або списків контролю доступу ACL.

Переваги DAC — гнучкість і простота реалізації. Недоліки — низький рівень централізованого контролю, високий ризик несанкціонованого розповсюдження прав доступу.

1.3.2. Мандатна модель MAC

MAC використовується у системах з підвищеними вимогами до безпеки (наприклад, у військових або фінансових установах). Кожному об'єкту та суб'єкту присвоюється рівень секретності.

Доступ дозволяється лише у випадку, якщо рівень суб'єкта відповідає або перевищує рівень об'єкта [2].

Переваги MAC — високий рівень безпеки, централізований контроль. Недоліки — складність адміністрування, негнучкість при зміні організаційних ролей.

1.3.3 Аналіз рольової моделі керування доступом RBAC

Рольова модель RBAC передбачає, що доступ користувачів визначається через ролі, які відповідають їх посадовим функціям.

Основні компоненти RBAC є користувачі Users, ролі Roles, дозволи Permissions, сесії Sessions.

Переваги RBAC в централізованому керуванні правами, зменшенню кількості помилок адміністрування, відповідність принципу найменших привілеїв Least Privilege.

Недоліки RBAC це статичність — ролі часто не враховують контекст (час, місце, пристрій), складність масштабування у великих організаціях із численними ролями.

У сучасних умовах класична RBAC доповнюється механізмами динамічного призначення ролей, які враховують поведінкові характеристики користувачів або контекст сесії [3].

1.3.4. Аналіз атрибутно-орієнтованої моделі керування доступом ABAC

Модель ABAC приймає рішення на основі множини атрибутів, які описують користувача відділу, рівень доступу, сертифікати, ресурс тип даних, власник, критичність, середовище час, місце, тип пристрою, рівень ризику.

ABAC надає високу гнучкість і масштабованість, оскільки правила можна формувати у вигляді логічних політик Policy Rules. Основний виклик — складність формалізації політик і високі вимоги до обчислювальних ресурсів.

1.4 Сутність динамічного призначення ролей у системах керування доступом

Динамічне призначення ролей Dynamic Role Assignment — це підхід до керування доступом, за якого права користувача визначаються не лише статичною роллю, а й контекстом використання системи, поточними

умовами, поведінковими характеристиками або результатами аналітики ризиків.

Мета такого підходу — забезпечення адаптивного рівня безпеки без зниження продуктивності користувачів.

У традиційній моделі RBAC ролі визначаються адміністратором і залишаються незмінними доти, поки не відбудуться зміни в організаційній структурі. Проте сучасні підприємства працюють у динамічних умовах — з тимчасовими командами, віддаленими працівниками, інтегрованими сервісами, де жорстко зафіксовані ролі стають обмеженням. Тому динамічне призначення ролей дозволяє автоматично коригувати права доступу залежно від контексту діяльності користувача, часу доби або місця входу типу пристрою, рівня ризику або довіри, поведінкових патернів користувача [4].

1.5. Огляд сучасних методів динамічного призначення ролей

У наукових дослідженнях і практиці інформаційної безпеки розрізняють кілька підходів до динамічного керування ролями.

1. Контекстно-орієнтовані моделі Context-Aware RBAC

Розширюють класичну модель RBAC, додаючи параметри контексту — час, місцезнаходження, тип операції. Переваги: збереження сумісності з RBAC, легке впровадження. Недоліки: обмежена адаптивність — контекст визначається наперед.

2. Атрибутно-рольові моделі Hybrid RBAC-ABAC

Поєднують переваги RBAC та ABAC. Ролі призначаються на основі множини атрибутів користувача (посада, рівень доступу, геолокація тощо). Переваги: висока гнучкість, масштабованість, можливість автоматизації. Недоліки в складності формування політик і потреба у значних обчислювальних ресурсах.

3. Поведінкові моделі Behavioral Role Mining

Використовують методи машинного навчання для аналізу історії дій користувачів з метою автоматичного визначення ролей або виявлення аномалій.

Переваги: самонавчання системи, здатність до адаптації.

Недоліком є потреба у великих обсягах навчальних даних та регулярному оновленні моделей.

4. Ризик-орієнтовані моделі Risk-Based Access Control

Рішення про призначення ролі приймається з урахуванням оцінки ризику конкретної сесії доступу. Наприклад, користувачу може бути тимчасово знижено рівень доступу при підозрілій активності.

Переваги в підвищенні безпеки, контекстна адаптація.

Недоліки в складності розрахунку ризику в реальному часі.

1.6. Використання машинного навчання в динамічному призначенні ролей

Методи машинного навчання (ML) активно застосовуються для автоматичного аналізу поведінкових даних користувачів і виявлення закономірностей у використанні прав доступу.

Основні підходи.

Кластеризація K-Means, DBSCAN — для групування користувачів за схожими діями та автоматичного формування ролей.

Класифікація Decision Tree, Random Forest — для прогнозування, яку роль слід призначити користувачу на основі історичних даних.

Аномалійний аналіз Isolation Forest, Autoencoder — для виявлення підозрілої поведінки, що не відповідає звичній ролі користувача.

Використання ML дозволяє створити адаптивну систему керування доступом, що динамічно змінює права користувача у реальному часі на основі аналізу його поведінки, знижуючи ризик внутрішніх загроз і людських помилок. В табл. 1.1 наведено Порівняльний аналіз підходів до динамічного призначення ролей.

Таблиця 1.1

Порівняльний аналіз підходів до динамічного призначення ролей

Підхід	Гнучкість	Масштабованість	Безпека	Реакція на зміни	Складність впровадження
Context-Aware RBAC	Середня	Висока	Середня	Обмежена	Низька
Hybrid RBAC-ABAC	Висока	Висока	Висока	Висока	Середня
Behavioral Role Mining	Дуже висока	Середня	Висока	Висока	Висока
Risk-Based Control	Висока	Середня	Дуже висока	Дуже висока	Висока

Як видно з таблиці, найбільш перспективними є гібридні та поведінкові моделі, які поєднують переваги ролей, атрибутів та аналітичних методів. Саме вони дозволяють реалізувати динамічне, контекстно-залежне призначення ролей, що відповідає вимогам сучасних підприємств [5].

1.7 Постановка задачі дослідження

Метою даного дослідження є розробка методів динамічного призначення ролей у системі керування доступом підприємства з використанням елементів машинного навчання, що забезпечить підвищення гнучкості, безпеки та адаптивності системи.

Для досягнення поставленої мети необхідно вирішити такі завдання.

1. Проаналізувати існуючі підходи до керування доступом RBAC, ABAC, гібридні моделі.
2. Визначити критерії ефективності динамічного призначення ролей.
3. Розробити концептуальну модель адаптивної системи керування доступом.
4. Реалізувати алгоритм динамічного призначення ролей із використанням ML-методів.
5. Провести експериментальну перевірку та оцінку ефективності розробленого підходу.

Висновки до розділу 1

У розділі розглянуто основні теоретичні підходи до побудови систем керування доступом.

Аналіз показав, що традиційні моделі DAC, MAC, RBAC, ABAC мають певні обмеження щодо динамічності та контексту прийняття рішень.

В умовах сучасних підприємств із гібридними інформаційними середовищами найбільш перспективними є динамічні моделі керування доступом, що поєднують рольові принципи RBAC з атрибутно-контекстним аналізом ABAC і підтримуються алгоритмами машинного навчання для адаптації до змін поведінки користувачів.

У розділі проаналізовано сучасні моделі та методи динамічного призначення ролей у системах керування доступом.

Показано, що класичні підходи RBAC, ABAC є недостатньо гнучкими для динамічного середовища сучасних підприємств.

Запропоновано використання гібридної архітектури з елементами машинного навчання, що забезпечує адаптивне керування доступом у режимі реального часу.

На основі проведеного аналізу сформульовано постановку задачі дослідження, яка передбачає створення моделі та програмного прототипу системи динамічного призначення ролей.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ІС ДИНАМІЧНОГО ПРИЗНАЧЕННЯ РОЛЕЙ У СИСТЕМАХ КЕРУВАННЯ ДОСТУПОМ ПІДПРИЄМСТВА

2.1 Концепція системи

Концепція розроблюваної системи ґрунтується на принципах адаптивного керування доступом, що враховує контекст взаємодії користувача з інформаційними ресурсами підприємства. На відміну від традиційних моделей, де ролі визначаються та призначаються статично, запропонована система передбачає автоматичне формування та оновлення ролей відповідно до поведінкових характеристик, ризикових факторів та актуальних бізнес-процесів [6].

Контекстна оцінка запитів доступу. Система використовує інформацію про час, локацію, тип пристрою, характер запиту, минулі дії користувача та поточний статус задач для визначення рівня ризику при отриманні доступу. Така оцінка дозволяє адаптувати призначення ролей у реальному часі.

Динамічне формування ролей. На основі контекстних даних та політик безпеки система автоматично модифікує набір дозволів, що надаються користувачу. Ролі формуються не лише на основі організаційної структури, а й на підставі фактичних сценаріїв взаємодії користувача із системою.

Аналіз поведінкових патернів. В основі системи лежать методи поведінкової аналітики, які дозволяють визначати типові й атипові дії користувачів. Виявлення аномалій сприяє автоматичному зниженню рівня доступу або ініціюванню додаткової автентифікації.

Інтеграція з корпоративними службами безпеки. Система підтримує взаємодію з існуючими механізмами авторизації LDAP, Active Directory, IAM-платформи, розширюючи їх функціональність за рахунок динамічної моделі ролей.

Політики адаптивного доступу. Ключовим компонентом є набір політик, що регламентують, як саме повинні змінюватися дозволи при зміні контексту. Політики можуть бути статичними (задано адміністраторами) або генерованими автоматично на основі машинного навчання.

Архітектурна концепція

Система складається з таких основних модулів як модуль автентифікації та первинної ідентифікації, що відповідає за базове підтвердження особи. Модуль збору контекстних даних, який отримує інформацію про параметри середовища. Аналітичний модуль поведінки користувачів, що виконує аналіз подій, класифікацію дій і виявлення аномалій. Модуль динамічного формування ролей, який на основі політик безпеки та аналітичних висновків формує актуальний набір дозволів. Модуль керування політиками, що забезпечує централізоване управління правилами доступу та їх автоматичне оновлення. Модуль інтеграції, який забезпечує обмін даними з корпоративними системами та сховищами.

Очікувані результати від впровадження це

1. зменшення ризику надмірних дозволів;
2. оперативне реагування на порушення безпеки;
3. зниження навантаження на адміністраторів систем доступу;
4. підвищення адаптивності системи до змін у бізнес-процесах;
5. покращення аудиту та відповідності стандартам безпеки.

Система динамічного призначення ролей, рисунок 2.1, — це інтелектуальна підсистема керування доступом, яка адаптивно формує права користувачів на основі аналізу контекстних параметрів, поведінкових даних та політик безпеки підприємства. Вона замінює традиційне статичне рольове керування доступом (RBAC) на більш гнучку, ризик-орієнтовану модель.

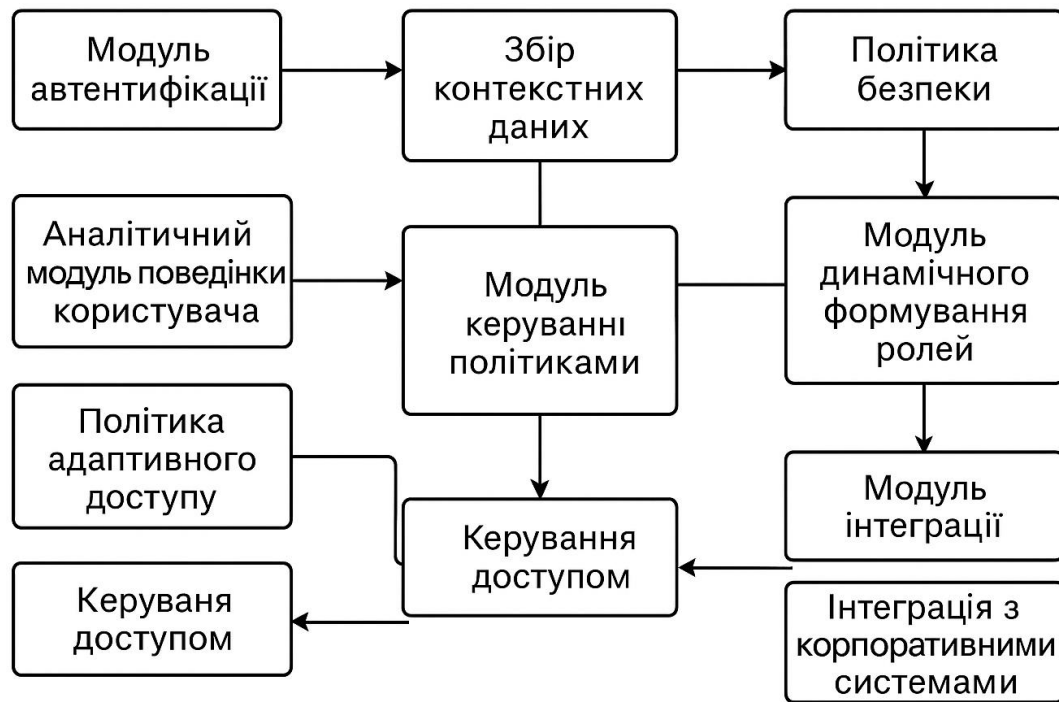


Рисунок 2.1 - Система динамічного призначення ролей

Модуль автентифікації, цей компонент виконує початкову перевірку особи користувача. Після успішної автентифікації система отримує унікальний ідентифікатор користувача та передає його до модулів збору контексту та поведінкової аналітики.

Модуль збору контекстних даних, виконує збір параметрів, необхідних для оцінки ризику доступу, а саме локація користувача, час доступу, тип і характеристика пристрою, важливість ресурсу, до якого здійснюється запит, попередні дії користувача. Ці контекстні дані використовуються для прийняття рішень щодо можливого тимчасового розширення або зменшення ролей.

Аналітичний модуль поведінки користувача, в основі модуля — методи машинного навчання та поведінкової аналітики. Завдання модуля виявлення аномальних дій, виявлення відхилень від звичайних патернів роботи, присвоєння користувачам поведінкового ризикового коефіцієнта. У разі підозрілої активності система може зменшити рівень доступу, вимагати додаткову автентифікацію або сповістити службу безпеки.

Модулем управління політиками є центральний елемент системи, який отримує дані з контекстного та поведінкового модулів. Порівнює їх із політиками безпеки. Приймає рішення щодо ролей користувачів. Генерує нові правила динамічного доступу.

Політики можуть бути як статичними — визначені адміністраторами, так і динамічними — сформовані системою на основі аналізу поведінки та ризиків.

Політика безпеки і політика адаптивного доступу включає набір правил, що визначають які дії дозволено певним ролям. Які умови вважаються ризиковими. Які зміни потрібно застосовувати при виникненні аномалій. Адаптивні політики дозволяють системі автоматично змінювати дозволи в режимі реального часу.

Модуль динамічного формування ролей функціонує на основі висновків аналітичних модулів та політик безпеки система. Формує поточний набір дозволів для користувача. Додає або видаляє ролі. Відстежує історію змін доступу. Забезпечує мінімальну необхідність вручну втручатися адміністраторам.

Модуль інтеграції забезпечує зв'язок з корпоративними системами LDAP/Active Directory, ERP/CRM, SIEM та інші системи безпеки. Він передає інформацію про сформовані ролі до зовнішніх систем авторизації [7].

Модуль керування доступом це фінальний компонент, який застосовує отримані ролі, надає або блокує доступ до ресурсів, веде журнал аудиту.

Цей модуль забезпечує повну відповідність рішень системи корпоративним політикам безпеки.

Переваги системи в адаптації до динамічних умов бізнес-процесів. Зменшенні ризику надмірних дозволів (over-privilege). Автоматизації значної частини адміністративної роботи. Підвищенням точності виявлення аномалій користувачів. Підвищення рівня кібербезпеки підприємства.

2.3 Архітектура системи

Архітектура DRAS, рисунок 2.2, побудована на модульному підході та забезпечує інтеграцію з існуючими інформаційними системами підприємства, системами аутентифікації, журналами подій та корпоративними сервісами. Вона включає такі основні компоненти.

1. Модуль аутентифікації Authentication Layer. Відповідає за перевірку особи користувача перед тим, як йому буде надано доступ до системи. Підтримує SSO Single Sign-On, LDAP/Active Directory, OAuth2/OpenID Connect. Після успішної аутентифікації передає у DRAS унікальний ідентифікатор користувача.

2. Контекстний модуль збору атрибутів Context & Attribute Collector. Цей модуль збирає різні атрибути, які використовуються для динамічного визначення ролей. Атрибути користувача посада, відділ, рівень доступу, статус працівника, сертифікації або дозволи.

Контекстні атрибути Context Awareness фактичне місцезнаходження офіс / VPN / заборонена зона, час доби, пристрій та його рівень безпеки, оцінка ризику активності користувача risk score, поведінкові показники behavior analytics. Модуль може отримувати дані з HR-систем, SIEM, корпоративних БД, від систем контролю доступу та мережевих інструментів безпеки.

3. Правильовий рушій Policy Decision Point – PDP. Центральний логічний компонент, де відбувається аналіз правил. Рушій містить політики доступу RBAC-політики (ролі за посадою), ABAC-політики (доступ за атрибутами), контекстні політики динамічна зміна ролей залежно від ризику, ситуаційні політики тимчасове підвищення або зниження ролі.

Механізм обчислення ролі відбувається на основі всіх атрибутів PDP. Формує актуальний профіль користувача, аналізує правила, визначає яку роль присвоїти в поточних умовах.

4. Модуль призначення ролей Policy Enforcement Point – PEP отримує рішення від PDP та призначає або відкликає роль у реальному часі, передає

дозволи та обмеження у бізнес-додатки, синхронізує зміни через API з корпоративними системами, PER реалізує контроль доступу на практиці.

5. Модуль аудиту та журналювання Audit & Monitoring Layer

Відповідає за повну прозорість і контроль роботи системи. Журнали включають історію призначення ролей, спрацьовування правил безпеки, аналіз аномалій та інцидентів, інтеграцію з SIEM для подальшої обробки. Цей модуль дозволяє у режимі реального часу контролювати всі зміни рівнів доступу.

6. Модуль аналітики та машинного навчання опціонально, але характерний для сучасних систем. Функції формування профілів поведінки користувачів, прогнозування ризикових активностей, рекомендації щодо оптимізації ролей, автоматичне створення "найменших необхідних" ролей Least Privilege. Модель постійно навчається на історичних даних.

7. API-шлюз та інтеграційні інтерфейси забезпечують взаємодію DRAS із ERP, CRM, банківськими системами, документообігом, системами контролю фізичного доступу, хмарними сервісами. API дозволяє швидко підключати нові підсистеми та розширювати функціональність.

8. База даних ролей, атрибутів та політик зберігає каталог ролей, атрибути користувачів, контекстні дані, правила динамічного призначення, журнали аудиту, БД структурована таким чином, щоб підтримувати як RBAC, так і ABAC моделі.

Система визначає роль автоматично — залежно від атрибутів і контексту. Рівень доступу може змінюватися в реальному часі — наприклад, при підвищенні ризику або зміні місцезнаходження. Підвищується безпека — мінімізація надмірних прав і загроз інсайдерських атак. Покращується керування доступом у складних корпоративних структурах.

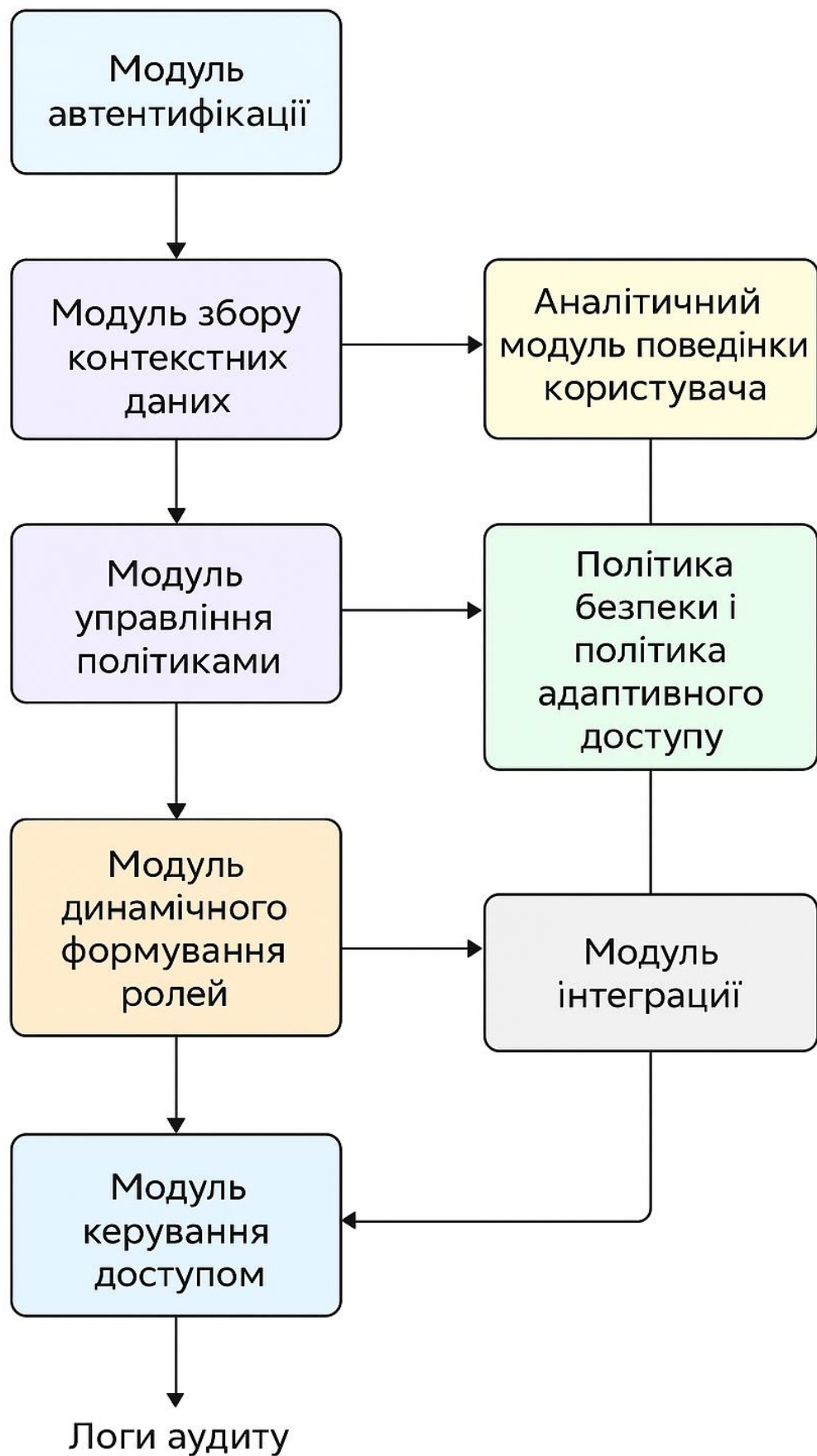


Рисунок 2.2 - Архітектура системи

2.3 Загально системні рішення

Основні актори:

Користувач Employee / User

Працівник підприємства, який проходить аутентифікацію та отримує доступ до корпоративних систем.

Адміністратор безпеки Security Administrator

Відповідальний за налаштування політик, контроль системи та аналіз журналів.

HR-система

Постачає атрибути працівника посада, відділ, статус.

Система аутентифікації SSO / AD / IAM

Проводить ідентифікацію та верифікацію користувача.

Бізнес-додатки / корпоративні сервіси

Споживають інформацію про роль, щоб вирішити: надати чи обмежити доступ.

SIEM / Система моніторингу безпеки

Отримує журнали подій і поведінкову інформацію.

Головні варіанти використання.

1. “Аутентифікація користувача”

Актори користувач, система аутентифікації.

Користувач вводить свої облікові дані. Система аутентифікації перевіряє їх та передає ідентифікатор у систему динамічного призначення ролей.

2. “Збір атрибутів користувача”

Актори HR-система, SIEM, система аутентифікації.

Модуль збору атрибутів отримує дані про посаду, відділ, статус, місцезнаходження, рівень ризику, тип пристрою та контекстні параметри.

3. “Обчислення ролі користувача динамічне призначення”

Немає зовнішніх акторів виконується PDP.

Правиловий рушій Policy Decision Point аналізує політики та атрибути і визначає, яку роль (або набір ролей) має отримати користувач у поточних умовах.

4. “Призначення ролі”

Актори бізнес-додатки, система керування доступом.

Модуль PER отримує рішення про роль та застосовує його в корпоративних системах надає дозвіл, обмежує доступ, відкликає роль, якщо змінюється контекст.

5. “Моніторинг активності користувача”

Актори SIEM.

Збирається інформація про поведінку користувача, яка може вплинути на роль (наприклад, підвищення рівня ризику).

6. “Автоматична зміна ролі під час ризиків”

Актори SIEM / модуль поведінкового аналізу.

При виявленні аномалій (підозріла активність, вхід з невідомого пристрою, нетипова поведінка) система автоматично знижує або змінює роль користувача.

7. “Перегляд журналів та аудиту”

Актори адміністратор безпеки.

Адміністратор переглядає історію змін ролей, події, аномалії, спрацьовування політик та проводить аналіз інцидентів.

8. “Налаштування політик призначення ролей”

Актор адміністратор безпеки.

Адміністратор створює або змінює правила RBAC/ABAC, задає контекстні параметри, визначає тригери для автоматичного корегування ролей.

Взаємозв'язки варіантів використання, рисунок 2.3, “Аутентифікація користувача” включає “Збір атрибутів користувача”. “Збір атрибутів” включає дані з HR-системи та SIEM. “Обчислення ролі” залежить від зібраних атрибутів. “Призначення ролі” наслідуює рішення PDP. “Моніторинг

активності” може викликати “Автоматичну зміну ролі”. “Налаштування політик” впливає на всі процеси обчислення та призначення ролей. “Перегляд журналів” отримує дані з усіх попередніх варіантів.

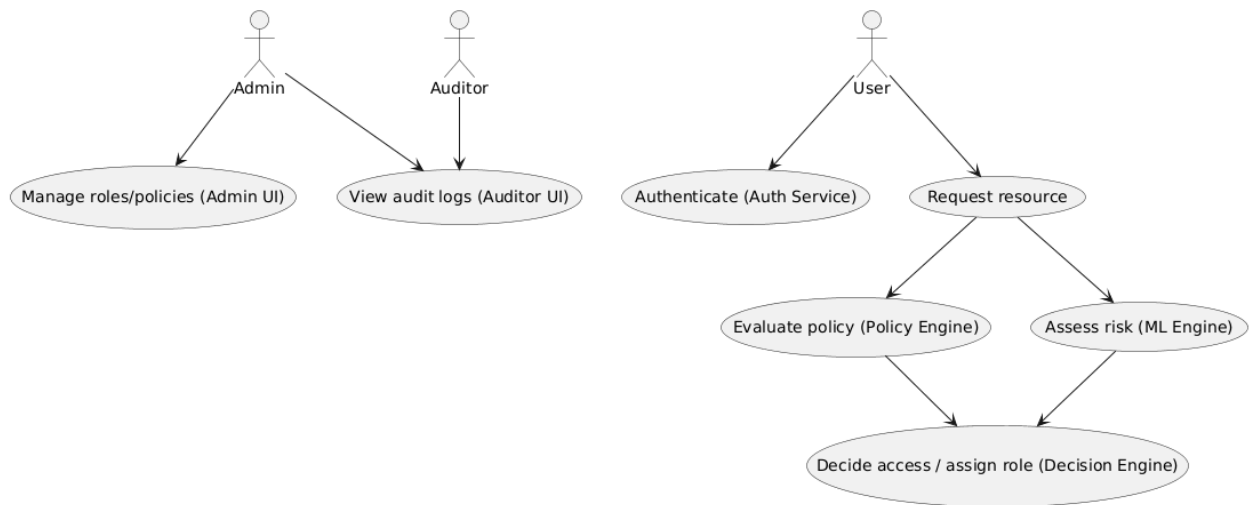


Рисунок 2.3 – Діаграма варіантів використання

2.4 Статична структура системи

Класова діаграма відображає статичну структуру системи, її основні сутності (класи), їх атрибути та взаємозв’язки. Вона моделює декларативні елементи системи такі як політики доступу, ролі, атрибути користувачів, логіку обробки та взаємодію між компонентами, див.рис.2.4.

1. Клас User (Користувач)

Представляє суб’єкта доступу — працівника підприємства.

Атрибути.

UserID int

FullName string

Department string

Position string

RiskLevel int

Status string (активний, відпустка, заблокований)

Методи GetAttributes(), UpdateRiskLevel()

Зв’язки.

1..* → має багато UserAttribute

1..* → пов'язаний із багатьма AssignedRole

2. Клас UserAttribute (Атрибут користувача)

Містить контекстні або статичні характеристики користувача.

Атрибути.

AttributeID int

Name string

Value string

Type string (статичний/динамічний)

Зв'язки багато → 1 User

3. Клас Role (Роль)

Описує набір дозволів для доступу до ресурсів.

Атрибути.

RoleID int

RoleName string

Description string

Зв'язки:

1..* → містить багато Permission

1..* → пов'язана з багатьма PolicyRule

4. Клас AssignedRole (Призначена роль)

Декларативна сутність, що фіксує факт призначення ролі користувачу.

Атрибути.

AssignmentID int

UserID int

RoleID int

ContextState string

AssignedAt datetime

ValidUntil datetime

Зв'язки багато → 1 User, багато → 1 Role

5. Клас Permission (Дозвіл)

Частина моделі керування доступом.

Атрибути.

PermissionID int

Resource: string

Action: string

Зв'язки багато → 1 Role, 6. Клас PolicyRule (Правило політики)

Основний декларативний елемент системи динамічного призначення ролей.

Атрибути.

RuleID int

Condition: string (логічний вираз ABAC/RBAC/контексту)

RoleID int

Priority: int

Методи. Evaluate(attributes: List<UserAttribute>): bool

Зв'язки багато → 1 Role

Використовується класом PolicyEngine

7. Клас PolicyEngine (Політичний рушій / PDP)

Приймає рішення про призначення ролі.

Атрибути.

EngineID int

Методи EvaluatePolicies(User): List<Role>, ResolveConflicts(),
SelectRole()

Зв'язки 1 → багато PolicyRule. Взаємодіє з User, UserAttribute, Role,
AssignedRole

8. Клас AuditLog (Журнал аудиту)

Фіксує всі операції із призначення ролей.

Атрибути.

LogID int

UserID int

Event string

Timestamp datetime

Details string

Методи WriteEvent()

9. Клас ContextMonitor (Модуль моніторингу контексту)

Відстежує ризики, аномалії та поведінку.

Атрибути.

MonitorID int

Методи CollectSignals(), DetectAnomaly(), UpdateUserRiskLevel()

Зв'язки Взаємодіє з User, PolicyEngine

Основні зв'язки між класами

User — 1.. UserAttribute*

User — 1.. AssignedRole — 1.. Role**

Role — 1.. Permission*

Role — 1.. PolicyRule*

*PolicyRule — ..1 PolicyEngine

PolicyEngine — створює/оновлює → AssignedRole

AuditLog — фіксує → всі зміни

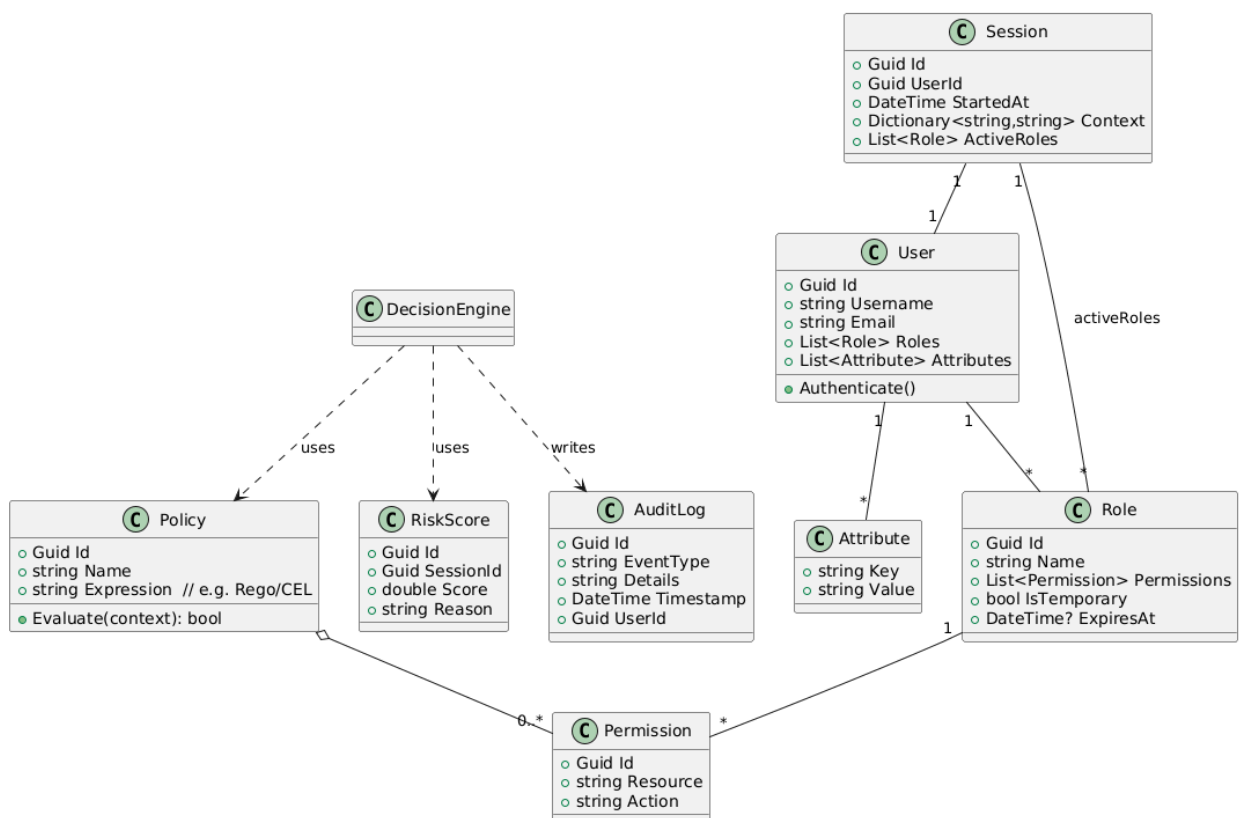


Рисунок 2.4 – Діаграма класів

2.5 Діаграма послідовності

Діаграма послідовності відображає кроки, які відбуваються під час обробки запиту користувача на доступ до ресурсу. Учасниками взаємодії є User, Access Gateway, Context Monitor, Policy Engine, Policy Repository, Role Manager, Audit Log, Resource Server.

1. Ініціація запиту доступу User надсилає запит на доступ до певного ресурсу (наприклад, документа, сервісу, модуля). Запит надходить до компонента Access Gateway, який обробляє всі вхідні запити авторизації.

2. Збір контекстних даних. Access Gateway звертається до Context Monitor із запитом отримати актуальні контекстні атрибути користувача місцезнаходження, час, тип активності, рівень ризику, можливі аномалії поведінки.

Context Monitor аналізує доступні дані, виконує перевірку на аномалії, оновлює значення ризику користувача та повертає набір атрибутів.

3. Оцінювання політик Access Gateway передає зібрані атрибути до Policy Engine (політичного рушія). Policy Engine надсилає запит до Policy Repository для отримання правил політик, пов'язаних із доступом до відповідного ресурсу. Policy Repository повертає список правил політик (Policy Rules), що можуть бути застосовані.

Policy Engine виконує процедуру оцінювання умов кожного правила, визначення релевантних ролей, резолюції конфліктів між політиками. У результаті Policy Engine формує рішення — яку роль або набір ролей слід призначити користувачу для цього запиту.

4. Призначення ролей Policy Engine передає рішення до Role Manager. Role Manager створює або оновлює запис про призначення ролі для користувача (Assigned Role) з урахуванням часу дії ролі, контексту, ризикового профілю. Інформація про призначення ролі записується у Audit Log.

5. Прийняття рішення про доступ Role Manager повертає сформовану роль назад до Access Gateway. Access Gateway на основі ролі перевіряє

дозволи (Permissions), пов'язані з роллю. Якщо дозволи відповідають запиту, Access Gateway надсилає команду до Resource Server про надання доступу. Resource Server надає доступ або повертає відмову.

6. Фіксація результату Access Gateway надсилає подію до Audit Log, де реєструється хто звертався, до чого, яка роль була призначена, рішення (доступ дозволено/відхилено). User отримує відповідь про результат авторизації.

Система використовує динамічні атрибути та контекст для адаптивного рішення. Ролі призначаються не статично, а в момент запиту, що підвищує безпеку. Усі дії прозоро фіксуються в журналі аудиту. Рішення формується на основі набору політик, що дозволяють реагувати на зміни поведінки користувача.

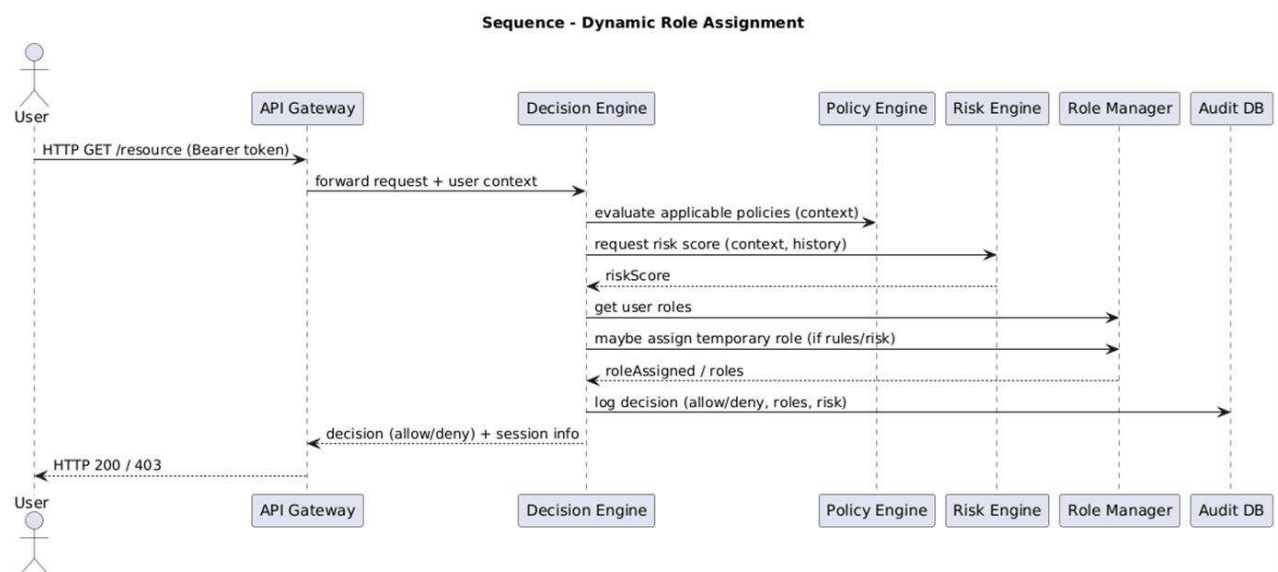


Рисунок 2.5 – Діаграма послідовності

2.6 Проєктування бази даних системи

1. Логічна модель даних (Logical Data Model), рисунок 2.6, описує сутності, атрибути та зв'язки між ними без прив'язки до конкретної СУБД. Вона відображає концептуальну структуру системи управління доступом, що підтримує динамічне призначення ролей.

Основні сутності

1. User (Користувач)

Описує суб'єктів, які ініціюють запити доступу.

Атрибути:

UserID (PK)

Login

FullName

Email

Department

Status (active/blocked)

2. Role (Роль)

Визначає набір повноважень і правил, які можуть бути призначені користувачу.

Атрибути:

RoleID (PK)

RoleName

RoleType (static, dynamic)

Description

3. Permission (Дозвіл)

Описує доступ до конкретної дії або ресурсу.

Атрибути:

PermissionID (PK)

PermissionName

ObjectType (file, service, module)

Operation (read, write, execute)

4. RolePermission (Зв'язок роль-дозвіл)

Зв'язує ролі з дозволами (зв'язок багато-до-багатьох).

Атрибути:

RoleID (FK)

PermissionID (FK)

5. ContextAttribute (Контекстний атрибут)

Зберігає параметри, що впливають на динамічне визначення ролі.

Атрибути:

ContextID (PK)

UserID (FK)

AttributeName

AttributeValue

Timestamp

6. Policy (Політика доступу)

Формалізовані правила, що використовуються в Policy Engine.

Атрибути:

PolicyID (PK)

PolicyName

ConditionExpression (логічний вираз)

Description

Priority

7. PolicyRole (Зв'язок політика–роль)

Вказує, яку роль може призначити політика.

Атрибути:

PolicyID (FK)

RoleID (FK)

8. AssignedRole (Призначена роль)

Фіксує результат динамічного призначення.

Атрибути:

AssignmentID (PK)

UserID (FK)

RoleID (FK)

ValidFrom

ValidTo

ContextSnapshot (збережений стан атрибутів)

9. AuditLog (Журнал подій)

Записує всі дії системи та рішення щодо доступу.

Атрибути:

LogID (PK)

UserID (FK)

ActionType

Resource

RoleAssigned

Decision (allow/deny)

Timestamp

RiskLevel

Зв'язки між сутностями

User — AssignedRole (1:M)

User — ContextAttribute (1:M)

Role — AssignedRole (1:M)

Role — RolePermission (1:M)

Permission — RolePermission (1:M)

Policy — PolicyRole (1:M)

User — AuditLog (1:M)

Role — AuditLog (1:M)

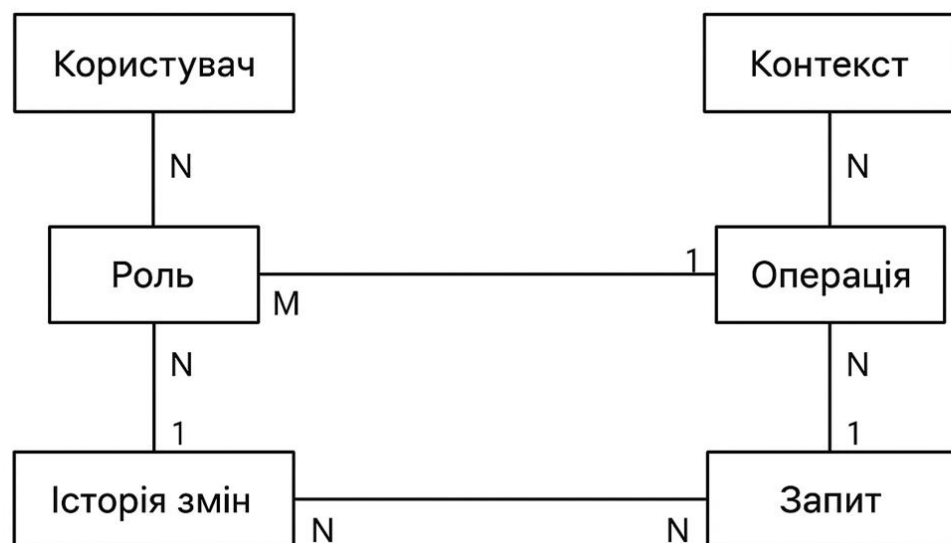


Рисунок 2.6 – Логічна модель БД

Фізична модель даних (Physical Data Model), рисунок 2.7, визначає структуру таблиць, типи даних, індекси, а також способи оптимізації для конкретної СУБД (наприклад, PostgreSQL).

Нижче представлено типовий варіант фізичного проєктування.

1. Таблиця Users

```
Users(  
    UserID SERIAL PRIMARY KEY,  
    Login VARCHAR(64) UNIQUE,  
    FullName VARCHAR(128),  
    Email VARCHAR(128),  
    Department VARCHAR(64),  
    Status VARCHAR(16)  
)
```

Індекси:

```
UNIQUE(Login)  
INDEX(Department)
```

2. Таблиця Roles

```
Roles(  
    RoleID SERIAL PRIMARY KEY,  
    RoleName VARCHAR(64),  
    RoleType VARCHAR(16),  
    Description TEXT  
)
```

3. Таблиця Permissions

```
Permissions(  
    PermissionID SERIAL PRIMARY KEY,  
    PermissionName VARCHAR(128),  
    ObjectType VARCHAR(32),  
    Operation VARCHAR(32)  
)
```


4. Таблица RolePermission

```
RolePermission(  
    RoleID INT REFERENCES Roles(RoleID),  
    PermissionID INT REFERENCES Permissions(PermissionID),  
    PRIMARY KEY (RoleID, PermissionID)  
)
```

5. Таблица ContextAttributes

```
ContextAttributes(  
    ContextID SERIAL PRIMARY KEY,  
    UserID INT REFERENCES Users(UserID),  
    AttributeName VARCHAR(64),  
    AttributeValue VARCHAR(256),  
    Timestamp TIMESTAMP  
)
```

Індекси:

```
INDEX(UserID, Timestamp)
```

6. Таблица Policies

```
Policies(  
    PolicyID SERIAL PRIMARY KEY,  
    PolicyName VARCHAR(128),  
    ConditionExpression TEXT,  
    Description TEXT,  
    Priority INT  
)
```

7. Таблица PolicyRole

```
PolicyRole(  
    PolicyID INT REFERENCES Policies(PolicyID),  
    RoleID INT REFERENCES Roles(RoleID),  
    PRIMARY KEY (PolicyID, RoleID)  
)
```

8. Таблица AssignedRoles

```
AssignedRoles(  
    AssignmentID SERIAL PRIMARY KEY,  
    UserID INT REFERENCES Users(UserID),  
    RoleID INT REFERENCES Roles(RoleID),  
    ValidFrom TIMESTAMP,  
    ValidTo TIMESTAMP,  
    ContextSnapshot JSONB  
)
```

Індекси:

```
INDEX(UserID)
```

```
INDEX(RoleID)
```

```
INDEX(ValidTo)
```

9. Таблица AuditLog

```
AuditLog(  
    LogID SERIAL PRIMARY KEY,  
    UserID INT REFERENCES Users(UserID),  
    ActionType VARCHAR(64),  
    Resource VARCHAR(128),  
    RoleAssigned VARCHAR(128),  
    Decision VARCHAR(16),  
    RiskLevel INT,  
    Timestamp TIMESTAMP  
)
```

Індекси:

```
INDEX(UserID)
```

```
INDEX(Timestamp)
```

```
INDEX(Decision)
```

```
INDEX(RiskLevel)
```

Логічна й фізична моделі забезпечують підтримку динамічного призначення ролей, зберігання контексту в режимі реального часу, застосування політик динамічного доступу, прозорий аудит усіх рішень.

Система реалізує RBAC → ABAC → DRBAC (Dynamic Role-Based Access Control).

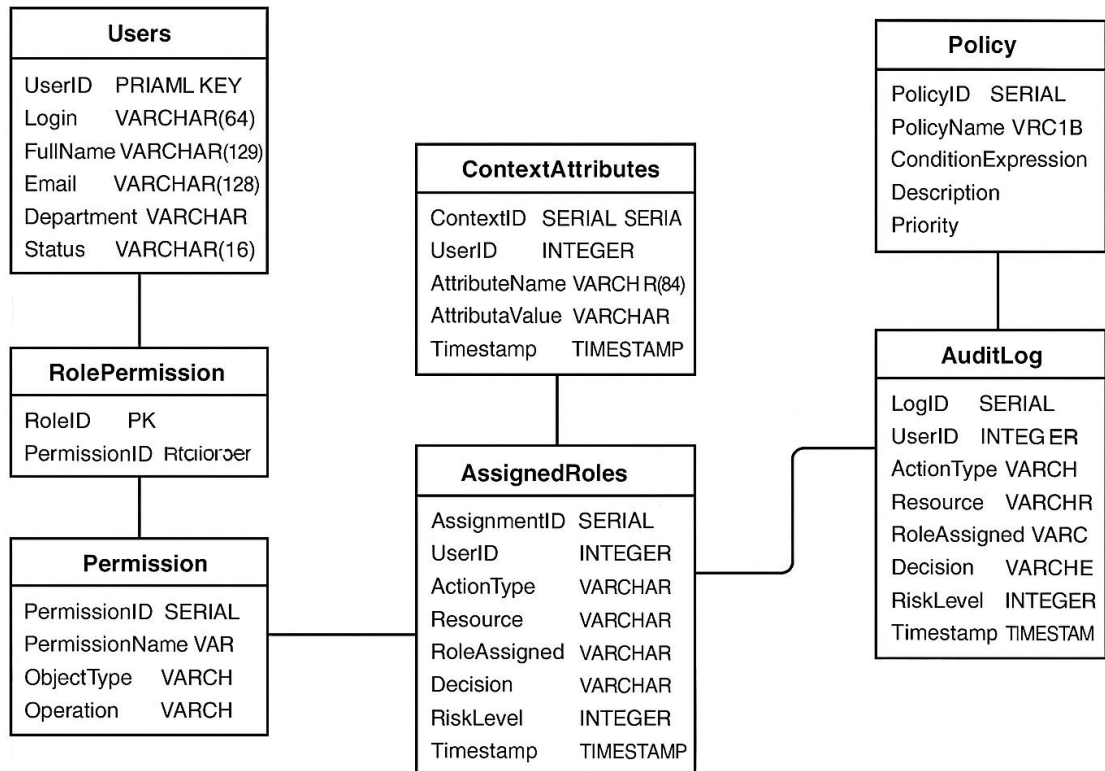


Рисунок 2.7 – Фізична модель БД

Висновки до розділу 2

У розділі було здійснено комплексне проектування інформаційної системи динамічного призначення ролей, що дало змогу сформулювати цілісне уявлення про її функціональну, логічну та технічну організацію. На основі аналізу предметної області визначено ключові вимоги до системи, зокрема: необхідність адаптивного контролю доступу, оперативного реагування на зміну поведінкових та контекстних факторів, інтеграції з існуючою інфраструктурою підприємства та забезпечення високого рівня інформаційної безпеки.

Проектування охопило створення структурно-функціональної схеми, діаграм варіантів використання, послідовності, класів, а також логічної та фізичної моделей даних. Отримані моделі продемонстрували, що запропонована система має модульну архітектуру, яка включає підсистеми автентифікації, моніторингу контекстних параметрів, аналізу ризиків, динамічного призначення ролей і аудиту доступу. Між компонентами встановлено чіткі інформаційні зв'язки, що забезпечує узгодженість оброблення даних та надійність прийняття рішень щодо доступу.

Логічна та фізична моделі даних показали можливість масштабування системи, забезпечення ефективного зберігання і швидкого отримання інформації, а також гарантували підтримку механізмів відстеження подій та формування історичних записів для подальшого аналізу. Структура БД є оптимізованою для реалізації адаптивного керування доступом і підтримує розширення новими параметрами поведінкових характеристик.

Таким чином, результати розділу підтверджують, що розроблена архітектура є цілісною, обґрунтованою та такою, що задовольняє вимоги сучасних систем безпеки. Запропоноване проєктне рішення закладає підґрунтя для подальшого етапу — реалізації та тестування системи динамічного призначення ролей, а також її інтеграції з інфраструктурою підприємства.

РОЗДІЛ 3. РОЗРОБКА ІС ПРИЗНАЧЕННЯ РОЛЕЙ

3.1 Фізичне розгортання системи

Для відображення фізичного розташування програмних компонентів системи динамічного призначення ролей на апаратних вузлах підприємства та взаємодію між ними проектуємо діаграму розгортання. Архітектура має багаторівневу структуру та складається з кількох основних вузлів.

1. Клієнтський вузол (Client Node) на клієнтських пристроях (ПК користувачів, ноутбуки, робочі станції) розгорнуто Web-інтерфейс системи керування доступом. Розміщений у браузері, реалізує сценарії перегляду доступів, підтвердження дій, авторизації, отримання повідомлень про зміну ролі.

API-клієнт використовує HTTPS для взаємодії з сервером застосунків, передає запити на автентифікацію, оцінку контексту, виконання операцій. Клієнтський вузол не містить бізнес-логіки — лише відображає дані та ініціює запити.

2. Сервер застосунків (Application Server) основний обчислювальний вузол, на якому розгорнуті компоненти такі як

2.1. Модуль автентифікації та авторизації (Auth Service)

Обробляє логін/лог-аут, токени доступу, взаємодіє з LDAP/AD (за потреби). Передає інформацію про користувача до модуля аналізу контексту.

2.2. Модуль динамічного призначення ролей (Dynamic Role Assignment Engine) в якому ключовими компонентами є системи аналізує контекст (місцезнаходження, час, тип дії, аномальність поведінки), виконання алгоритму визначення ролі, тимчасового підвищення/пониження повноважень, фіксування зміни у журналі безпеки.

2.3. Контекстний аналізатор (Context Analyzer) отримує дані від зовнішніх сенсорів, логів, історії дій користувача застосовує правила (rule-based). Передає результат у "Dynamic Role Assignment Engine".

2.4. Бізнес-логіка керування доступами (Access Controller) порівнює призначену роль із дозволами системи, приймає рішення дозволити операцію, або відхилити або зафіксувати подію як підозрілу.

2.5. Лог сервер (Logging & Auditing Service) записує події змін ролей, аномалії, спроби доступу, контекстні фактори. Усі ці компоненти взаємодіють між собою через внутрішню шину або REST API.

3. Сервер бази даних (Database Server) на окремому фізичному або віртуальному вузлі розміщено реляційна база даних, репозиторій моделей поведінки, інтеграційний вузол.

3.1. Реляційна база даних містить таблиці користувачів, ролі та їх ієрархію, контекстні параметри, журнали дій, логіку збережених процедур (за потреби).

3.2. Репозиторій моделей поведінки (Behaviour Model Store) зберігає профілі користувачів, історичні дії, патерни ризикової поведінки. Компоненти серверу застосунків здійснюють доступ до БД через внутрішній захищений канал.

4. Інтеграційний вузол (External Services Node) містить зовнішні сервіси та корпоративні системи Active Directory / LDAP — джерело базових даних про користувачів. SIEM-система — отримує події безпеки. VPN/Firewall — надає дані про підозрілу активність. Взаємодія відбувається через API або secure connectors. Канали зв'язку між клієнтом і сервером застосунків HTTPS (TLS). Між сервером застосунків і БД: захищений внутрішній канал, VLAN або SSH-тунель. Між сервером застосунків та зовнішніми сервісами API + шифрування. Усі канали відповідають вимогам інформаційної безпеки. Текстовий опис діаграми розгортання демонструє чітку логіку взаємодії компонентів, розподіл функцій між вузлами, фізичну структуру системи, взаємозв'язки, потрібні для роботи динамічного призначення ролей, відповідність вимогам безпеки підприємства.

3.2 Вимоги до апаратного забезпечення для розробки системи

Для забезпечення ефективного функціонування середовища розробки, тестування та часткового моделювання навантаження інформаційної системи були визначені мінімальні та рекомендовані вимоги до апаратного забезпечення.

1. Мінімальні вимоги

Мінімальні характеристики забезпечують можливість розробки, запуску та початкового тестування компонентів системи без значних затримок.

Робоча станція розробника включає процесор 4-ядерний CPU, рівень Intel Core i3 / AMD Ryzen 3. Оперативна пам'ять 8 GB RAM. Накопичувач HDD або SSD обсягом від 256 GB. Відеокарта інтегрована, з підтримкою Full HD. Мережа з доступом до інтернету 10–20 Мбіт/с.

Також клавіатура, миша, мікрофон, вебкамера для роботи з репозиторіями та командною взаємодією.

2. Рекомендовані вимоги для комфортної роботи з ML-модулями, контейнерами, емуляторами та серверними сервісами. Робоча станція розробника. Процесор 6–8 ядер, Intel Core i5 / i7 або AMD Ryzen 5 / 7. Оперативна пам'ять 16–32 GB RAM. Накопичувач SSD від 512 GB NVMe бажано. Відеокарта дискретна VIDIA GTX 1650 або вище — прискорення ML-модулів. Мережа - стабільний інтернет 50–100 Мбіт/с. Монітор від 24", роздільна здатність 1920×1080 або більше.

3. Серверне апаратне забезпечення для тестування та моделювання роботи системи. Мінімальна конфігурація тестового сервера це процесор 4 ядра Intel Xeon E3 / AMD EPYC Entry. Оперативна пам'ять 8–16 GB. Накопичувач SSD 256 GB. Мережа 1 Gbps внутрішня, 50–100 Мбіт/с зовнішня. Рекомендована конфігурація процесора 8–12 ядер Intel Xeon Silver / AMD EPYC. Оперативна пам'ять 32 GB. Накопичувач SSD NVMe 512 GB. Мережеві можливості 1–10 Gbps. Можливість розгортання контейнеризації

Docker / Kubernetes / Azure Container Apps. Підтримка віртуалізації: Intel VT-x або AMD-V

4. Апаратні вимоги для компонентів ML-обробки оскільки система використовує алгоритми динамічного призначення ролей, аналіз поведінки та аномалій, для їх навчання бажана наявність прискорення.

ML-станція опційно для навчання моделей. Процесор 8+ ядер. Оперативна пам'ять 32–64 GB. GPU - NVIDIA серії RTX 3060/3070/4060 або вище. Накопичувач SSD NVMe 1 TB. Охолодження підвищена ефективність для тривалих обчислень.

5. Периферійне та додаткове обладнання. ДБЖ для забезпечення безперебійної роботи сервера. Маршрутизатор з підтримкою VLAN/Firewall для тестування безпеки. Зовнішні носії (SSD/HDD) для резервного копіювання

3.3 Вимоги до програмного забезпечення

1. Операційна система

Для розробки, тестування та розгортання системи можуть використовуватися такі ОС Windows 10/11 (64-bit) або Windows Server 2019/2022 — основне середовище для .NET-застосунків. Linux (Ubuntu 20.04/22.04, Debian, CentOS) — для розгортання серверних компонентів, контейнеризації та CI/CD. macOS 12+ (опціонально) — для розробників, що працюють у кросплатформеному середовищі.

2. Середовище розробки (IDE) система повинна розроблятися з використанням сучасних середовищ Microsoft Visual Studio 2022 – основне IDE для .NET-розробки. Visual Studio Code – кросплатформенний редактор для легких модулів та мікросервісів. Підтримка C# 10/11, ASP.NET Core 6/7/8.

3. Серверна платформа та фреймворки такі як .NET 6/7/8 SDK – для створення веб-API, сервісів аналізу політик і обробки контекстних даних. ASP.NET Core Web API – для реалізації інтерфейсів взаємодії компонентів системи. Entity Framework Core – для доступу до бази даних та ORM.

4. База даних підтримувані СУБД Microsoft SQL Server. PostgreSQL – для контейнеризованого та хмарного розгортання. SQLite – для розробки та тестування. Додаткові інструменти SQL Server Management Studio (SSMS) або pgAdmin — для адміністрування БД.

5. Засоби для моделювання та проєктування включають для побудови UML-діаграм та моделей даних Visual Paradigm, StarUML, Draw.io, Enterprise Architect. Підтримувані типи діаграм Use Case, Sequence, Class, Deployment, Activity. ER-діаграми для логічного та фізичного моделювання БД.

6. Засоби аналітики та машинного навчання, якщо система використовує аналіз ризиків чи поведінкове профілювання ML.NET – для реалізації моделей класифікації аномалій. TensorFlow.NET — опціонально для складніших моделей. Python + Jupyter Notebook — для попереднього експериментального аналізу.

7. Засоби безпеки та криптографії для реалізації авторизації, токенів і політик доступу OAuth 2.0 / OpenID Connect – стандарти автентифікації. IdentityServer4 / Duende IdentityServer — для управління токенами доступу. JWT Library for .NET — для створення токенів.

8. Засоби логування, моніторингу та аудиту Serilog, NLog — для логування подій доступу. Grafana + Prometheus — моніторинг активності (опційно). Elastic Stack (ELK) – для обробки логів великих систем.

9. Засоби контейнеризації та розгортання для розгортання серверної частини Docker, Docker Compose — контейнеризація сервісів. Kubernetes (Minikube, K3s) — для масштабування. GitHub Actions, GitLab CI/CD — автоматизація збірки.

10. Інструменти для тестування Postman або Insomnia — перевірка REST-API. Swagger UI / OpenAPI — документація API. xUnit, MSTest, NUnit — модульне тестування.

Програмне забезпечення повинно забезпечувати повний цикл розробки .NET-системи, підтримку моделювання політик доступу та ролей,

можливість інтеграції з аналітичними та ML-модулями, безпечне розгортання у хмарному або локальному середовищі.

Висновки до розділу 3

У третьому розділі було виконано проектування інфраструктури системи динамічного призначення ролей, що включало створення діаграми розгортання, визначення апаратних ресурсів та специфікацію програмного забезпечення, необхідного для реалізації та функціонування системи.

Розроблена діаграма розгортання дала змогу визначити структурну взаємодію між серверами, клієнтськими пристроями, компонентами мережевої інфраструктури та модулями системи безпеки. На основі аналізу було сформовано оптимальну конфігурацію: сервер автентифікації, сервер політик, база даних, сервер моніторингу контексту та клієнтські робочі станції. Архітектура забезпечує відмовостійкість, масштабованість і можливість інтеграції з корпоративними системами управління доступом.

У межах проектування визначено також вимоги до апаратного забезпечення, що враховують обчислювальні потреби алгоритмів оброблення контекстних даних, роботи політичного рушія та функціонування сервісів моніторингу. Рекомендовано використання багатоядерних процесорів, достатнього обсягу оперативної пам'яті та високопродуктивних засобів зберігання, що дозволяють підтримувати реєстрацію подій у режимі реального часу та обробку ризикових показників користувачів.

Окремо були сформульовані вимоги до програмного забезпечення, що включають використання серверного середовища з підтримкою мікросервісної архітектури, систем управління базами даних, інструментів логування, модулів для аналізу поведінкових атрибутів та платформ для розгортання політик доступу. Також визначено потребу у підтримці сучасних фреймворків, протоколів безпеки, стандартів шифрування та сервісів контейнеризації.

Таким чином, у розділі комплексно сформовано техніко-архітектурні передумови для реалізації системи. Розроблені рішення забезпечують

надійність, безпечність та адаптивність системи динамічного призначення ролей, що створює міцне підґрунтя для її подальшої реалізації, тестування та впровадження в корпоративне середовище.

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ РОЗРОБКИ

Створення системи динамічного призначення ролей у системах керування доступом підприємства є доцільним як з технічної, так і з економічної точки зору. У цьому розділі проведено аналіз ефективності впровадження розробленої системи, визначено очікувані витрати, користь, а також оцінено окупність та перспективи експлуатації.

4.1 Обґрунтування технічної необхідності

Традиційні моделі керування доступом, які використовують статичне призначення ролей, не відповідають сучасним вимогам безпеки. Вони не враховують контекстні параметри (місцезнаходження, час, поведінкові аномалії), що створює високі ризики несанкціонованого доступу. Технічна необхідність розробки системи зумовлена такими факторами.

- зростанням кількості кіберзагроз, що потребують адаптивних систем контролю доступу;
- необхідністю автоматизації прийняття рішень на основі політик безпеки;
- потребою у скороченні ручних операцій з призначення ролей адміністраторами;
- вимогами стандартів інформаційної безпеки (ISO/IEC 27001, NIST SP 800-53), які рекомендують контекстно-орієнтоване керування доступом.

Розроблена система технічно здатна інтегруватися з існуючими інформаційними ресурсами підприємства та забезпечує високий рівень масштабованості, надійності та стійкості.

4.2 Розрахунок витрат на розробку системи

Структура витрат включає.

4.2.1 Витрати на оплату праці розробників

У типових умовах до проєкту залучаються:

Посада	Кількість	Тривалість	Ставка (грн/місяць)	Вартість (грн)
Програміст .NET	1	2 місяці	35 000	70 000
Інженер з безпеки	1	1.5 місяця	40 000	60 000
Аналітик	1	1 місяць	30 000	30 000
Тестувальник	1	1 місяць	25 000	25 000
Разом витрати на персонал: 185 000 грн				

4.2.2 Витрати на інфраструктуру та середовище розробки

Найменування	Вартість, грн
Хмарний сервер (2 місяці × 800 грн/міс)	1 600
Ліцензійні інструменти (IDE, CI/CD), за потреби	3 000
Тестове середовище	1 500
Разом витрати 6 100 грн	

4.2.3 Загальна собівартість розробки

Сумарні витрати $185\,000 + 6\,100 = 191\,100$ грн

4.3 Економічна ефективність впровадження

Для підприємства впровадження системи дає такі переваги:

4.3.1 Прямі економічні вигоди

Зменшення навантаження на ІТ-персонал — економія близько 20 год/місяць адміністратора доступів (приблизно 6 000 грн/міс).

Скорочення інцидентів безпеки — середня вартість інциденту може перевищувати 50 тис. грн; система дозволяє знизити ризик на 60–70%.

Автоматизація рутинних процесів, що скорочує час на onboarding/offboarding співробітників.

4.3.2 Непрямі вигоди

Підвищення інформаційної безпеки підприємства. Підвищення рівня відповідності стандартам безпеки. Покращення керованості інфраструктури. Можливість масштабування і подальшої інтеграції з SIEM/IDM системами.

4.4 Розрахунок окупності

Припустимо, що прямі щомісячні вигоди становлять економія часу ІТ-персоналу: 6 000 грн/міс, зниження вартості наслідків інцидентів (оцінка) 10 000 грн/міс.

Сумарна вигода 16 000 грн/міс.

Окупність $191\,100 \text{ грн} / 16\,000 \text{ грн} \approx 12$ місяців.

Таким чином, система повністю окупасться приблизно за **1 рік експлуатації**.

Висновки з техніко-економічного обґрунтування

Розробка системи динамічного призначення ролей є економічно доцільною та технічно обґрунтованою. Вона дозволяє підприємству зменшити ризики несанкціонованого доступу. Автоматизувати рольове керування доступом. Скоротити витрати на ручні операції. Підвищити відповідність вимогам міжнародних стандартів безпеки. Отримати довгостроковий економічний ефект.

Впровадження системи забезпечує значний рівень окупності та підвищує загальну ефективність роботи підприємства.

РОЗДІЛ 5 ОХОРОНА ПРАЦІ

5.1. Значення охорони праці в діяльності фахівця з інформаційних технологій

Охорона праці є важливою складовою забезпечення безпечних умов діяльності працівників підприємства, зокрема спеціалістів з інформаційних технологій. Незважаючи на те, що професія ІТ-фахівця не належить до категорії підвищено небезпечних, робота за комп'ютером супроводжується низкою професійних ризиків: тривалим статичним навантаженням, можливими порушеннями зору, надмірним психоемоційним напруженням, впливом електромагнітних полів, неналежними умовами мікроклімату. Тому організація безпечних і комфортних умов праці суттєво впливає на продуктивність персоналу та якість створюваних інформаційних систем, включаючи систему динамічного призначення ролей.

5.2. Аналіз небезпечних і шкідливих факторів на робочому місці

Під час розробки та експлуатації інформаційних систем до потенційно небезпечних і шкідливих факторів належать фізичні фактори, недостатня або надмірна освітленість, шум і вібрації від офісної техніки, електромагнітне випромінювання від моніторів та мережевого обладнання, статична електрика, нерациональний мікроклімат (температура, вологість, вентиляція).

Психофізіологічні фактори статичне навантаження при сидячій роботі. Монотонність та висока інтенсивність розумових процесів, тривала напруга зорового аналізатора, високий рівень стресу під час розробки та тестування систем безпеки.

Електротехнічні фактори робота з обладнанням, що живиться від електромережі 220 В, можливість короткого замикання, пожежі або ураження електричним струмом.

5.3. Вимоги до організації робочого місця розробника

Для забезпечення безпечного виконання робіт рекомендується дотримання таких норм:

Робочий стіл і крісло регульована висота крісла та спинки, наявність підлокітників. Висота столу — 680–800 мм відповідно до стандартів ДСТУ. Достатній простір для ніг (не менше 600 × 500 мм).

Розміщення монітора відстань до очей — 50–70 см. Верхня частина екрана має знаходитися на рівні очей або трохи нижче. Екран не повинен створювати відблисків.

Клавіатура та маніпулятор клавіатура має розташовуватися на відстані 10–30 см від краю столу. Використання ергономічної миші або трекпада.

Освітлення комбіноване: загальне + місцеве. Рівень освітленості для роботи за ПК — не менше 300–500 лк. Уникнення прямих світлових потоків на екран.

Мікроклімат температура — 18–24 °С. Відносна вологість — 40–60%. Наявність вентиляції або кондиціонування.

Режим праці перерви кожні 60 хв роботи за ПК (5–10 хв). Загальна тривалість роботи за комп'ютером не повинна перевищувати 6 годин на день без додаткових перерв.

5.4. Електробезпека при роботі з комп'ютерним обладнанням

Для попередження ураження електричним струмом усе обладнання має бути заземленим. Використання стабілізаторів напруги та мережевих фільтрів. Розміщення кабелів у кабель-каналах для уникнення механічних пошкоджень. Лаборона роботи з відкритими корпусами системних блоків під напругою. Дотримання вимог ПУЕ та ПБЕ при експлуатації комп'ютерної техніки.

5.5. Пожежна безпека у приміщенні розробників

У приміщенні необхідно забезпечити наявність вогнегасників порошкових або вуглекислотних. Справну систему протипожежної сигналізації. Використання негорючих матеріалів для обробки. Відсутність перевантаження електромережі. Зберігання вільного доступу до евакуаційних виходів.

Особливу увагу слід приділяти серверній кімнаті, де розміщується система керування доступом.

5.6. Вимоги безпеки під час роботи з даними та інформаційними ресурсами

Оскільки розроблювана система стосується управління доступом, додатково враховуються вимоги інформаційної безпеки використання складених і регулярно змінюваних паролів. Багатофакторна аутентифікація. Шифрування передавання та зберігання службових даних. Регулярне резервне копіювання. Навчання персоналу щодо виявлення фішингових атак та соціальної інженерії.

5.7. Заходи з охорони праці під час розробки програмного забезпечення

Під час роботи над системою динамічного призначення ролей застосовуються такі заходи використання ліцензійного та надійного програмного забезпечення. Організація безпечного доступу до репозиторіїв коду. Дотримання стандартів безпечної розробки OWASP, NIST. Періодичний аудит коду і тестування безпеки. Забезпечення зручного та безпечного робочого середовища для команди.

Висновки до розділу 5

У рамках розділу встановлено основні вимоги та заходи щодо охорони праці для спеціалістів, що здійснюють розробку і супровід системи динамічного призначення ролей у системах керування доступом підприємства. Аналіз показав, що робота ІТ-фахівця містить ряд небезпечних і шкідливих факторів, однак їх вплив може бути мінімізований шляхом правильного облаштування робочого місця, забезпечення відповідного мікроклімату, організації режиму праці, дотримання вимог електробезпеки та пожежної безпеки.

Запропоновані заходи створюють умови для комфортної, продуктивної та безпечної праці розробника, що є важливою складовою успішної реалізації та впровадження розробленої інформаційної системи.

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

У сучасних умовах цифровізації підприємств важливим аспектом упровадження будь-яких інформаційних систем є дотримання вимог екологічної безпеки та мінімізація негативного впливу на навколишнє середовище. Розробка та експлуатація системи динамічного призначення ролей у системах керування доступом підприємства належить до екологічно безпечних видів діяльності, однак також потребує розгляду ресурсоспоживання, утилізації відходів електронного обладнання та енергоефективності ІТ-інфраструктури.

6.1. Екологічні аспекти використання комп'ютерної техніки

Функціонування розробленої системи передбачає використання серверного та мережевого обладнання, робочих станцій, засобів зберігання даних і периферійних пристроїв. Головні екологічні ризики, притаманні цим компонентам споживання електроенергії, утворення електронних відходів E-waste, використання витратних матеріалів акумуляторів, кабелів, пластикових компонентів, виділення тепла та необхідність додаткового кондиціонування серверних приміщень.

Для зменшення негативного впливу варто застосовувати обладнання з високим класом енергоефективності Energy Star, 80PLUS, використовувати SSD-накопичувачі замість HDD, а також оптимізувати навантаження на сервери за допомогою віртуалізації.

6.2. Оптимізація енергоспоживання та ресурсів

У межах проєкту пропонується використовувати наступні екологічно відповідальні підходи.

Використання хмарних технологій

Перенесення обчислювальних процесів у хмарні середовища знижує потребу підприємства у фізичних серверах, що зменшує споживання електроенергії та потребу в системах охолодження.

Віртуалізація та контейнеризація

Використання Docker, Kubernetes чи Hyper-V забезпечує більшу щільність розміщення сервісів на одному фізичному сервері, що знижує карбоновий слід.

Оптимізація обчислювальних процесів

Динамічні методи призначення ролей не потребують великих обсягів пам'яті чи графічних обчислень. Використання оптимізованих алгоритмів знижує CPU-навантаження.

Впровадження автоматичного вимикання неактивних компонентів

Сервери можуть переходити у режими зниженого енергоспоживання при відсутності запитів.

6.3. Управління електронними відходами

Під час експлуатації системи можливе накопичення електронних відходів (вийшли з ладу компоненти, кабелі, роутери, акумулятори). Відповідно до вимог екологічного законодавства, підприємство повинно здійснювати сортування електронних відходів і передавати їх ліцензованим підприємствам з утилізації. Забезпечувати безпечне зберігання несправного обладнання до моменту утилізації. Використовувати відповідні контейнери для збору батарейок, акумуляторів і блоків живлення. Уникати самостійного спалювання чи викидання електронних елементів у побутові відходи.

6.4. Вплив інформаційної системи на екологічну політику підприємства

Запропонована система безпосередньо не генерує екологічних ризиків, але сприяє зменшенню кількості паперових документів, оскільки всі процеси керування доступом стають цифровими, раціональному використанню ІТ-інфраструктури, завдяки можливості централізованого контролю доступу та мінімізації дублювання обчислювальних сервісів, збільшенню тривалості використання обладнання, оскільки навантаження на системи можна ефективно розподіляти завдяки моніторингу.

6.5. Дотримання екологічних стандартів та нормативів

Під час створення та експлуатації системи важливо враховувати вимоги таких нормативних документів Закон України «Про охорону навколишнього природного середовища». Закон України «Про відходи». ISO 14001 — міжнародний стандарт екологічного менеджменту. Директива ЄС WEEE щодо утилізації електричних та електронних відходів.

Запропонована система відповідає вимогам екологічної безпеки, оскільки не потребує спеціальних процесів, що можуть негативно вплинути на природу.

Висновки до розділу 6

Розробка системи динамічного призначення ролей є екологічно безпечною та не створює додаткових ризиків для довкілля. Використання сучасного енергоефективного обладнання, хмарних технологій та принципів відповідального поводження з електронними відходами забезпечує мінімальний вплив на навколишнє середовище. Реалізація системи сприятиме цифровій екологізації підприємства, знижуючи ресурсоемність процесів та підвищуючи раціональність використання ІТ-інфраструктури.

ВИСНОВКИ

У дипломній роботі проведено комплексне дослідження теоретичних, методологічних та практичних аспектів динамічного призначення ролей у системах керування доступом підприємства. На основі аналізу існуючих моделей RBAC, ABAC та їхніх адаптивних розширень було визначено ключові проблеми традиційних систем доступу, зокрема низьку гнучкість, складність підтримки, обмеженість реакції на контекстні зміни та підвищені ризики внутрішніх загроз.

У ході виконання роботи:

Проаналізовано сучасні методи контролю доступу, виявлено їхні переваги та недоліки, а також визначено актуальність переходу до інтелектуальних динамічних моделей призначення ролей на основі поведінкових та контекстних параметрів.

Сформовано концепцію адаптивної системи динамічного призначення ролей, що передбачає інтеграцію механізмів аналізу поведінки користувачів, контекстних тригерів та автоматизованих правил, які забезпечують оперативне коригування прав доступу згідно з ризиковим профілем користувача.

Розроблено архітектуру системи, яка включає модулі аутентифікації, управління ролями, поведінкової аналітики, обробки подій безпеки та інтеграційні компоненти. Архітектура забезпечує масштабованість, модульність та можливість інтеграції з корпоративною інфраструктурою.

Створено логічну та фізичну модель бази даних, що підтримує процеси зберігання користувацьких атрибутів, історії активності, контекстних параметрів та правил призначення ролей.

Спроектовано ключові діаграми UML (use case, class, sequence, deployment), що відображають поведінку і структуру системи, а також взаємодію її компонентів.

Розроблено прототип інформаційної системи, який демонструє роботу алгоритмів динамічного призначення ролей, обробку подій ризику та автоматичну зміну прав доступу відповідно до визначених правил.

Проведено техніко-економічне обґрунтування, яке засвідчує доцільність впровадження системи з погляду зменшення ризиків інформаційної безпеки, скорочення витрат адміністрування та підвищення рівня захищеності корпоративних ресурсів.

У результаті виконання роботи доведено, що використання методів динамічного призначення ролей є ефективним підходом до підвищення безпеки доступу в підприємствах із високою інтенсивністю інформаційних взаємодій. Запропонована система забезпечує адаптивність, автоматизацію та здатність реагувати на зміни контексту в реальному часі, що значно підвищує стійкість корпоративної інфраструктури до внутрішніх та зовнішніх загроз.

Отже, поставлена мета дипломної роботи досягнута, а отримані результати можуть бути використані для подальшої розробки повнофункціональних систем керування доступом нового покоління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3), 224–274.
- [2] Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., & Sandhu, R. (2015). Attribute-based access control. *IEEE Computer*, 48(2), 85–88.
- [3] Bertino, E., & Sandhu, R. (2005). Database security—Concepts, approaches, and challenges. *IEEE Transactions on Dependable and Secure Computing*, 2(1), 2–19.
- [4] Goyal, V., & Tripathi, A. (2020). Dynamic role-based access control model for cloud computing environment. *Journal of Information Security and Applications*, 55, 102676.
- [5] Alotaibi, B., & Alomar, N. (2022). Context-aware and risk-based access control for enterprise systems. *Computers & Security*, 116, 102660.
- [6] Liu, Q., Zhang, H., & Guo, Z. (2023). AI-driven adaptive access control in enterprise systems. *Information Systems Frontiers*, 25(4), 1251–1263.
- [7] Ажищев, В. Ф., Качурка, Д. І., Леус, С. О., & Морарь, М. І. (2025). Дослідження методів системи динамічного призначення ролей у системах керування доступом підприємства. У матеріалах VI Міжнародної науково-практичної інтернет-конференції «Інформаційні технології: моделі, алгоритми, системи (ITMAS – 2025)» (16–17 листопада 2025 р.). Миколаїв: НУК імені адмірала Макарова С. 245-247
<https://itconf.nuos.edu.ua/2025/publications/investigation-of-methods-for-dynamic-role-assignment-in-enterprise-access-control-systems/>

ДОДАТОК А - Технічне завдання

1. Загальні положення

Технічне завдання визначає вимоги до створення інформаційної системи (ІС) динамічного призначення ролей, яка забезпечуватиме адаптивний контроль доступу на основі контекстних, поведінкових та ризикових факторів. Система призначена для підвищення рівня інформаційної безпеки підприємства шляхом впровадження гнучких моделей авторизації.

Розробка виконується відповідно до вимог чинних стандартів у галузі інформаційних технологій та інформаційної безпеки.

2. Підстава для розробки

Навчальний план підготовки магістра за спеціальністю «Комп'ютерні науки». Завдання кафедри щодо виконання кваліфікаційної магістерської роботи. Внутрішні нормативи підприємств щодо модернізації систем керування доступом.

3. Мета розробки

Створення інформаційної системи, що реалізує методи динамічного призначення ролей (Dynamic Role Assignment) з використанням контекстно-залежного аналізу та механізмів оцінки ризиків для адаптивного контролю доступу користувачів до інформаційних ресурсів підприємства.

4. Завдання розробки

Дослідити сучасні методи керування доступом (RBAC, ABAC, Risk-Based Access Control).

Розробити адаптивну модель призначення ролей, що враховує контекст виконання операцій, поведінкові аномалії, рівень ризику користувача.

Створити архітектуру ІС з виділенням логічних модулів.

Розробити структурно-функціональну модель, діаграми UML, логічну та фізичну модель БД. Реалізувати прототип системи. Забезпечити можливість інтеграції із зовнішніми системами автентифікації.

Передбачити ведення журналу аудиту подій. Провести тестування та оцінити ефективність системи.

5. Вимоги до функціональних характеристик

Система повинна забезпечувати.

5.1. Функції користувача

Подання запиту на доступ до ресурсу.

Отримання дозволу або відмови.

Перегляд інформації про особисті сесії.

5.2. Функції адміністратора

Керування політиками доступу.

Додавання/редагування ресурсів.

Керування ролями та дозволами.

Перегляд журналів аудиту.

5.3. Функції системи

Автоматичний збір контекстних параметрів.

Аналіз поведінкових аномалій.

Обчислення ризикового профілю користувача.

Динамічне призначення ролей у момент запиту.

Прийняття рішення про доступ згідно з політиками.

Збереження подій контролю доступу.

6. Вимоги до надійності

Система має забезпечувати безперебійний доступ 24/7.

Відмова окремого модуля не повинна спричиняти зупинку всієї системи. Дані БД повинні зберігатися з використанням резервного копіювання. Журнал аудиту має бути захищений від модифікацій.

7. Вимоги до безпеки підтримка сучасних криптографічних протоколів передачі даних (TLS). Обов'язкова автентифікація користувачів. Захист від SQL-ін'єкцій, XSS, CSRF атак. Контроль спроб несанкціонованого доступу. Розмежування доступу відповідно до ролей.

8. Вимоги до апаратного забезпечення

Сервер (мінімальні характеристики):

CPU: 4 ядра,

RAM: 8–16 GB,

SSD: від 120 GB,

Gigabit Ethernet.

Робоча станція розробника:

CPU: 4 ядра,

RAM: ≥ 8 GB,

OC Windows / Linux.

9. Вимоги до програмного забезпечення

Операційна система: Windows 10+, Ubuntu 20+ або інші сумісні.

Середовище розробки: Visual Studio / Rider / VS Code.

База даних: MS SQL Server / PostgreSQL.

Фреймворки:

.NET 6/7,

ASP.NET Core,

бібліотеки для ML/аналізу аномалій (ML.NET).

Інструменти для моделювання: Draw.io / StarUML / Visual Paradigm.

10. Стадії та етапи розробки

Аналітичні дослідження предметної області.

Формування технічного завдання.

Проектування (UML, БД, архітектури).

Розробка модулів системи.

Тестування та апробація.

Підготовка експлуатаційної документації.

Захист магістерської роботи.

11. Порядок контролю та приймання роботи

Перевірка працездатності системи проводиться на тестових сценаріях.

Оцінюється відповідність функціоналу ТЗ.

Система передається замовнику у вигляді програмного продукту та документації.

12. Джерела розробки

Наукові публікації щодо RBAC, ABAC, policy-based access control.

Стандарти ISO/IEC 27001, 27002, 29146.

Документація .NET та ML.NET.

ДОДАТОК Б - Інструкція користувача

1. Загальні положення

Ця інструкція користувача призначена для ознайомлення з порядком роботи у системі динамічного призначення ролей, яка забезпечує адаптивне керування доступом до інформаційних ресурсів підприємства з урахуванням контекстних атрибутів, поведінкових факторів та політик безпеки.

Система надає змогу здійснювати автентифікацію та авторизацію користувачів, отримувати динамічно сформовану роль відповідно до контексту, переглядати власні доступи та історію авторизацій, адміністраторам — керувати політиками доступу, ролями та журналами подій.

2. Вимоги до користувача

Для роботи з системою потрібно наявний обліковий запис підприємства, доступ до корпоративної мережі або VPN, веббраузер (Google Chrome, Mozilla Firefox, Microsoft Edge).

3. Вхід до системи

Перейдіть за наданою адресою вебпорталу системи. Введіть логін та пароль корпоративного облікового запису. У разі увімкненої багатофакторної автентифікації виконайте додаткове підтвердження (SMS-код, мобільний додаток, токен). Після успішної автентифікації ви будете перенаправлені на головну сторінку.

4. Головне меню

Після входу користувач бачить такі основні розділи.

4.1. “Мій профіль” перегляд особистих даних користувача, перегляд активної динамічно призначеної ролі, історія авторизацій та рішень системи, поточний ризиковий рівень (низький / середній / високий).

4.2. “Мої доступи” список ресурсів, до яких наданий доступ, короткий опис прав доступу, термін дії тимчасових ролей.

4.3. “Повідомлення” сповіщення про підвищений ризик, повідомлення про зміну ролі, результати перевірок безпеки.

5. Функціонал адміністратора

Адміністратор має розширені можливості.

5.1. Політики доступу створення, редагування та видалення політик контролю доступу, налаштування умов: час, місце, поведінковий профіль, ризик, визначення ролей, які призначаються при виконанні умов.

5.2. Керування ролями створення статичних та динамічних ролей, прив'язка дозволів (permissions) до ролей, призначення базових ролей користувачам.

5.3. Контроль контексту перегляд згенерованих ризикових показників, відстеження аномалій користувачів, контроль активності у реальному часі.

5.4. Журнал аудиту перегляд повної історії подій доступу, фільтрація за користувачем, ресурсом, роллю, датою. Експорт подій у формат CSV / PDF.

6. Як формується роль у користувача система автоматично оцінює місцезнаходження під час запиту, частоту дій користувача, використання незвичних пристроїв, час доби, історію попередніх аномалій.

На основі політик система визначає дозволити доступ, надати іншу (підсилену/обмежену) роль, відмовити, запитати додаткову автентифікацію.

Користувач бачить у профілі призначену роль і причину її призначення.

7. Стандартний сценарій користувача

Користувач заходить у систему. Отримує контекстно згенеровану роль.

Переходить до потрібного корпоративного сервісу (CRM, окументообіг, файловий архів тощо). Система перевіряє необхідні дозволи.

У разі нестандартних дій користувач отримує сповіщення. Усі дії фіксуються в Audit Log.

8. Типові повідомлення системи "Доступ дозволено" – роль відповідає необхідним дозволам. "Недостатньо прав" – ваша роль не містить потрібних дозволів. "Ризиковий вхід. Потрібно пройти додаткову автентифікацію." "Призначено тимчасову роль" – роль активна протягом обмеженого часу. "Аномалія у поведінці: доступ обмежено".

9. Вихід із системи.

Для забезпечення безпеки рекомендується натиснути "Вийти" у верхньому правому куті, закрити браузер після роботи, не передавати облікові дані третім особам.

10. Заходи безпеки

Не використовуйте слабкі паролі. Не залишайте комп'ютер без нагляду під час активної сесії. Негайно звертайтеся до адміністратора при підозрі на компрометацію облікового запису. Використовуйте корпоративний VPN для віддаленої роботи.

11. Підтримка користувачів

У разі виникнення запитань або технічних збоїв звертайтеся до служби підтримки.

Email support@enterprise.ua

Тел.: +38 (099) 243-55-97

Графік роботи: 09:00–18:00 (Пн–Пт).

ДОДАТОК В - Екранні форми розробки

2. Вимоги до користувача

- Цілієвля осоеетниила
- Даступ сь д осацігала VPN
- Веб друзер (Google Chrome), Chrome, Microsoft Edge, Microsoft

3. Вхід до системи

Динамічне призначення ролей

Мій профіль

Мої доступи

Повідомлення

Мій Іванов

Оператор

Екстерний Росак

Исчегало

23.10.2023-30:22

Середній неаи

24.10.2023-12:18

Середній неаки

4. Головне меню

- Мій профіль — пероцап із ресионг ваїп
- Мої доступи — частопанувелпипия пизцнделл из потратн а еектоути
- Повідомлення — истрором сьлє пша срома ризи

5. Функціонал адміністратора

- Слослєзлалцєалістрисетоп
палкклм доступно
- Релматива роготопналвллшл ил
палвлонни тострли
- Гепелєдєдлгочл колслелел
- Пыдєстона ризолзалл

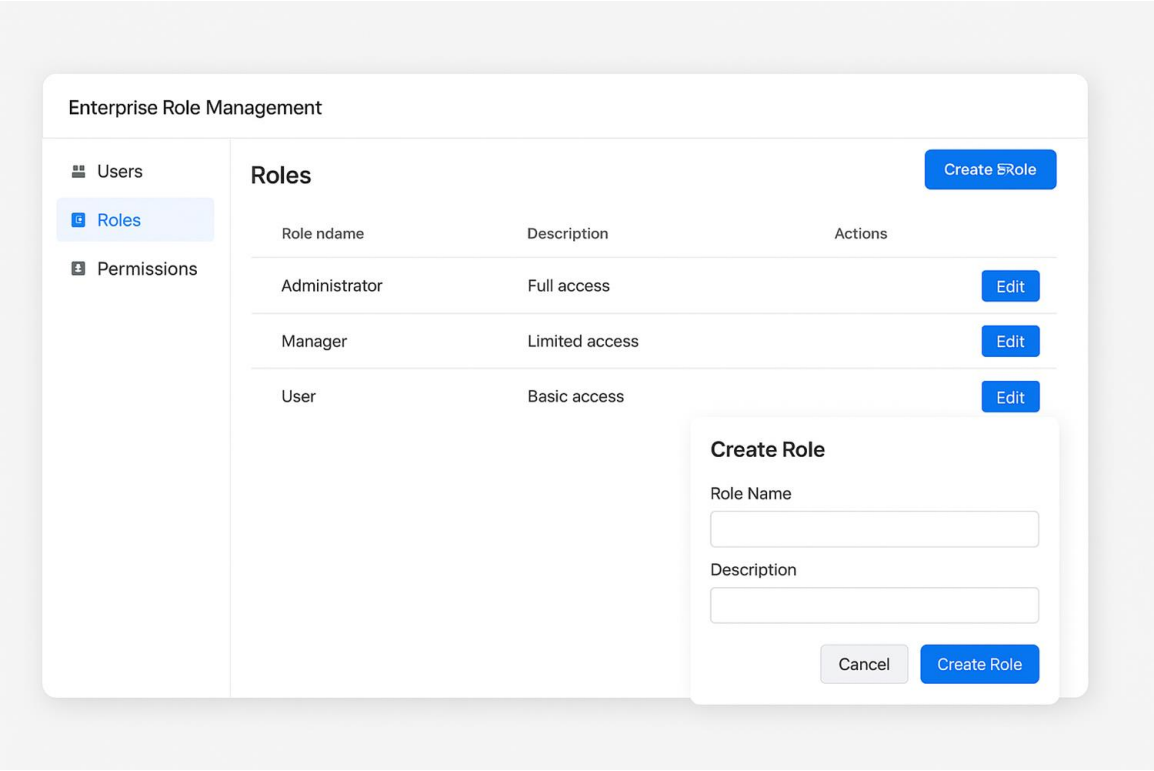
Мій профіль

Оператор

Оператор

Логін

Пароль



№	Назва тесту	Очікуваний результат	Результат
1	Вхід до системи	Успішний вхід	☒ Пройдено
2	Невірний пароль	Повідомлення про помилку	☒ Пройдено
3	Додавання користувача	Новий користувач доданий	☒ Пройдено
4	Призначення ролі вручну	Роль змінена	☒ Пройдено
5	Автоматичне призначення ролі	Роль змінюється автоматично	☒ Пройдено
6	Обмеження доступу	Access denied	☒ Пройдено
7	Формування звіту	Створено звіт PDF	☒ Пройдено
8	Перевірка навантаження	Час відповіді ≤ 1.5 с	☒ Пройдено
9	SQL Injection	Безпечна обробка вводу	☒ Пройдено
10	Зміна ролі під час сесії	Роль оновлено	☒ Пройдено

Результат тестування системи динамічного призначення ролей