

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА

«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

**на тему: «Налагоджування та тестування системи безпечного
управління привілейованим доступом (PAM) у хмарному
середовищі Microsoft 365»**

здобувача: Калініченка Данііла Костянтиновича _____

Науковий керівник: к.т.н. Гулак Н. К. _____

**Робота допущена до захисту перед екзаменаційною комісією з
атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА

«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО

Керівник проєктної групи (гарант)
освітньо-професійної програми
«Кібербезпека»

_____ к.е.н., проф. А.В. Бегун
_____ 2026

ЗАТВЕРДЖУЮ

Завідувач кафедри системного аналізу
та кібербезпеки

_____ д.ф.-м.н., проф. І.А. Джалладова
_____ 2026.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти: Калініченко Данііл Костянтинович
(прізвище, ім'я, по батькові)

_____ очної (денної) _____ форми навчання
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

на тему: « Налагоджування та тестування системи безпечного управління привілейованим доступом (PAM) у хмарному середовищі Microsoft 365»

Тему затверджено наказом ректора Університету від «___» _____ 20__ р. №__

Кваліфікаційна бакалаврська робота виконується на матеріалах літературних та інформаційних джерел з кібербезпеки та архітектури хмарних технологій, міжнародних стандартів інформаційної безпеки, офіційної технічної документації платформ Microsoft Entra ID та Microsoft 365, а також результатів практичного розгортання та експериментального тестування в ізольованому хмарному середовищі.

ПЛАН КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ РОБОТИ

Розділ 1	Аналіз загроз та концепцій управління доступом у хмарних середовищах
Розділ 2	Технологічні основи та інструменти Microsoft Entra ID для захисту доступу
Розділ 3	Практична реалізація системи PAM у середовищі підприємства.

Об'єкт дослідження	Процеси забезпечення інформаційної безпеки корпоративних хмарних інфраструктур та системи управління ідентифікаторами (Identity and Access Management).
Предмет дослідження	Методи, моделі, алгоритми та інструментальні програмні засоби безпечного управління привілейованим доступом у корпоративній хмарній інфраструктурі на базі платформи Microsoft 365.
Мета кваліфікаційної бакалаврської роботи	Захист критичних інформаційних ресурсів корпоративного хмарного середовища підприємства за рахунок проектування, автоматизованого розгортання та експериментального тестування комплексної системи динамічного контролю адміністративних повноважень на базі концепції нульової довіри.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1 «Аналіз загроз та концепцій управління доступом у хмарних середовищах»: Провести комплексний аналіз сучасного ландшафту кіберзагроз хмарним обліковим записам, дослідити архітектурні принципи побудови систем безпеки за концепцією нульової довіри (Zero Trust), виконати порівняльний аналіз наявних рішень класу Privileged Access Management та сформувані науково-технічне обґрунтування вибору платформи Microsoft 365 як базового середовища захисту.

У розділі 2 «Технологічні основи та інструменти Microsoft Entra ID для захисту доступу»: Дослідити внутрішню архітектуру платформи Microsoft Entra ID та формалізувати концептуальну модель управління на основі ролей, детально вивчити функціональні можливості сервісу Privileged Identity Management для динамічного виділення прав, проаналізувати логіку превентивного захисту через політики умовного доступу, а також дослідити криптографічні методи автентифікації та захисту від компрометації сесій.

У розділі 3 «Практична реалізація системи РАМ у середовищі підприємства»: Розробити програмні сценарії мовою PowerShell для автоматизованого розгортання об'єктів інфраструктури привілейованих груп та адміністративних одиниць, практично налаштувати хмарні політики динамічного виділення прав за принципом саме вчасно (Just-In-Time), впровадити інтелектуальний шлюз превентивної фільтрації контексту запитів із вимогою використання стійкої до фішингу апаратної автентифікації FIDO2, а також провести серію експериментальних тестів стійкості архітектури до компрометації з налаштуванням безперервного моніторингу подій у SIEM-системі Microsoft Sentinel.

Завдання підготував
науковий керівник

(підпис)

Гулак Н. К.
(прізвище, ініціали)

Завдання одержав
здобувач

(підпис)

Калініченко Д.К.
(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної бакалаврської роботи містить 56 сторінок, 13 рисунків, 7 таблиць, 40 джерел за переліком посилань та 3 додатки.

Об'єкт дослідження: процеси забезпечення інформаційної безпеки хмарних інфраструктур та систем управління ідентифікацією.

Мета кваліфікаційної роботи: захист ресурсів корпоративного хмарного середовища через розгортання системи динамічного контролю привілейованого доступу.

Методи дослідження: системний аналіз, моделювання загроз (STRIDE), конфігурування хмарних засобів, скриптова автоматизація.

У спеціальній частині дана характеристика сучасних векторів кібератак на ідентифікатори (AiTM, “втома MFA”) та принципів архітектури Zero Trust.

В роботі проведено аналіз політик умовного доступу, інструментів PAM та платформи Microsoft Entra ID.

Запропоновано багаторівневу модель управління доступом (Tiering Model) із застосуванням концепції Just-In-Time.

Побудовано комплексну превентивну систему захисту, що поєднує PIM, Conditional Access та апаратні ключі FIDO2.

Розроблено PowerShell-скрипти для автоматизованого розгортання привілейованих груп та JSON-конфігурації політик безпеки.

В економічному розділі визначено ефективність (TCO) нативного хмарного рішення, що оптимізує операційні витрати компанії на 35-45%.

Практичне значення роботи полягає у створенні комплексу, що повністю ліквідує постійні адміністративні права, зводячи їх активний час до нуля.

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані IT-підрозділами для стандартизованого впровадження захисту хмарних активів у середовищі Microsoft 365.

Наукова новизна дослідження полягає у вдосконаленні моделі доступу RBAC часовим вектором, що доводить зменшення вікна вразливості системи на 90-95%.

Напрямки подальших досліджень: машинне навчання для аналізу транзакцій та автоматизація реагування в SIEM Microsoft Sentinel.

Ключові слова: Інформаційна безпека, Microsoft 365, Microsoft Entra ID, Управління доступом, Zero Trust, Conditional access, Just-in-time.

ВІДГУК

на кваліфікаційну бакалаврську роботу

студента Калініченка Данііла Костянтиновича гр. ІК-402

на тему: «Налагоджування та тестування системи безпечного управління привілейованим доступом (PAM) у хмарному середовищі Microsoft 365»

Актуальність теми. Тема є надзвичайно актуальною з огляду на зростання кількості кіберінцидентів, спрямованих на хмарні ідентифікатори. Вразливість класичних підходів зі статичним наданням привілеїв робить перехід корпоративних інфраструктур на концепцію нульової довіри (Zero Trust) критично важливим завданням.

Повнота розкриття теми. Тема розкрита повністю. Робота містить ґрунтовне теоретичне обґрунтування, аналіз сучасного ландшафту хмарних загроз та глибоку практичну реалізацію інструментів управління доступом. Структура є логічною та повністю відповідає поставленим завданням.

Теоретичний рівень. Теоретична частина написана на високому рівні. Здобувач демонструє глибоке розуміння багаторівневих систем захисту (Tiering Model) та успішно застосовує математичний апарат для опису рольового доступу (RBAC). Огляд літератури міг би бути дещо ширшим у частині аналізу алгоритмів машинного навчання для виявлення аномалій.

Практична цінність полягає в розробці і впровадженні адаптивної моделі управління доступом методом найменших привілеїв для зниження ступеня ризиків для інформаційних систем за рахунок мінімізації часу існування активних адміністративних привілеїв до 0 в стані спокою.

Самостійність виконання роботи. Робота виконана повністю самостійно. Здобувач демонструє здатність до прийняття обґрунтованих технічних рішень. Архітектура динамічного розмежування прав Just-In-Time та написані JSON-конфігурації свідчать про глибоке осмислення проблематики, а не просте відтворення інструкцій.

Якість оформлення, загальна та спеціальна грамотність. Робота оформлена відповідно до вимог ДСТУ. Мова викладу є грамотною, спеціальна термінологія використовується доречно. Ілюстративний матеріал (блок-схеми, скріншоти) є вичерпним та належним чином підписаним.

Переваги та недоліки роботи. Головна перевага - потужна практична спрямованість та підтвердження результатів симуляціями хакерських атак. Позитивно відзначається техніко-економічне обґрунтування вибору платформи. Серед недоліків слід зазначити, що опис інтеграції з SIEM-системою Microsoft Sentinel міг би супроводжуватися більшою кількістю розроблених кастомних правил виявлення (KQL).

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК.

Кваліфікаційна бакалаврська робота виконана на високому рівні та повністю відповідає вимогам. Здобувач Калініченко Д. К. продемонстрував відмінну теоретичну підготовку та інженерні навички у сфері безпеки хмарних технологій. Робота заслуговує оцінку «відмінно», а її автор – на присвоєння кваліфікації «Бакалавр з кібербезпеки».

Науковий керівник к.т.н.

Доцент кафедри системного аналізу та кібербезпеки _____ Наталія ГУЛАК
 (посада) (підпис) (ім'я, прізвище)
 “ ” 2026 р.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу

студента Калініченка Данііла Костянтиновича гр. ІК-402

на тему: «Налагоджування та тестування системи безпечного управління привілейованим доступом (РАМ) у хмарному середовищі Microsoft 365»

Спеціальність: 125 «Кібербезпека»

Актуальність теми. В умовах міграції корпоративних інфраструктур у хмару класичний мережевий периметр втрачає ефективність. Зростання кількості атак на ідентифікатори робить використання статичних привілеїв критичною вразливістю. Впровадження систем РАМ на базі парадигми нульової довіри (Zero Trust) є одним із найпріоритетніших завдань для сучасного кіберзахисту.

Наукова новизна. Полягає у розробці багаторівневої архітектури розмежування повноважень (Tiering Model) в екосистемі Microsoft Entra ID із математично обґрунтованим застосуванням часових (Just-In-Time) та контекстних факторів для мінімізації площі поверхні атаки.

Практична цінність полягає в розробці і впровадженні адаптивної моделі управління доступом методом найменших привілеїв для зниження ступеня ризиків для інформаційних систем за рахунок мінімізації часу існування активних адміністративних привілеїв до 0 в стані спокою.

Якість проведеного аналізу. Аналітична частина виконана на високому рівні. Здобувач детально дослідив механіки сучасних атак (зокрема AiTM), порівняв локальні та хмарні підходи РАМ і навів переконливе техніко-економічне обґрунтування (ТСО) використання нативних засобів Microsoft 365.

Уміння користуватися літературними джерелами. Студент впевнено працює з фаховою літературою, міжнародними стандартами та офіційною документацією. Теоретичні моделі та вибір інструментарію мають належне бібліографічне підтвердження.

Якість оформлення, загальна та спеціальна грамотність. Робота оформлена акуратно, текст викладено технічно грамотною мовою з дотриманням академічного стилю. Спеціальна термінологія використовується доречно, а графічний матеріал є інформативним.

Переваги та недоліки. До безперечних переваг належить цілісність роботи: від побудови теоретичної моделі до тестування в умовах симуляції атак та налаштування моніторингу в Microsoft Sentinel. Серед недоліків слід зазначити фокусування виключно на екосистемі єдиного вендора. Робота виграла б від порівняння з альтернативними рішеннями (наприклад, CyberArk)

для оцінки ризиків вендорного блокування (vendor lock-in), однак це не знижує високої якості дослідження.

Загальний висновок і оцінка роботи. Кваліфікаційна бакалаврська робота Калініченка Д. К. є завершеним самостійним дослідженням, яке повністю відповідає вимогам до випускних робіт освітнього ступеня бакалавра. Здобувач продемонстрував високий рівень інженерної підготовки. Робота заслуговує на оцінку **«90/відміно/А»**, а Калініченко Д.К. – присвоєння кваліфікації «Бакалавр з кібербезпеки».

Рецензент к.т.н., доцент, Ільєнко Анна

Завідувач кафедри Кібербезпеки _____ Анна ІЛЬЄНКО

Національний університет «КАІ»

(посада)

(підпис)

(ім'я, прізвище)

Печатка

“ _____ ” _____ 2026 р.

Зміст

РОЗДІЛ 1 АНАЛІЗ ЗАГРОЗ ТА КОНЦЕПЦІЙ УПРАВЛІННЯ ДОСТУПОМ У ХМАРНИХ СЕРЕДОВИЩАХ.....	5
1.1 Класифікація загроз обліковим записам у хмарі	5
1.2. Концепція нульової довіри та роль РАМ у її реалізації.....	8
1.3. Порівняльний аналіз архітектури РАМ	11
1.4. Обґрунтування вибору Microsoft 365 як платформи захисту	14
1.5 Висновки до першого розділу.....	17
РОЗДІЛ 2 ТЕХНОЛОГІЧНІ ОСНОВИ ТА ІНСТРУМЕНТИ MICROSOFT ENTRA ID ДЛЯ ЗАХИСТУ ДОСТУПУ	19
2.1. Архітектура Microsoft Entra ID та концептуальна модель RBAC.....	19
2.2. Функціональні можливості Privileged Identity Management (PIM)	24
2.3. Політики умовного доступу як інструмент превентивного захисту	27
2.4. Методи автентифікації та захисту від компрометації облікових даних.....	28
2.5 Висновки до другого розділу	31
РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ РАМ У СЕРЕДОВИЩІ ПІДПРИЄМСТВА	33
3.1. Підготовка хмарної інфраструктури та базове налаштування середовища	33
3.2. Практичне налаштування політик керування привілейованими ідентифікаторами (PIM).....	36
3.3. Впровадження превентивного захисту через Conditional Access.....	40
3.4. Експериментальне тестування, моніторинг та оцінка ефективності	46
3.4 Висновки до третього розділу.....	49
ВИСНОВКИ	52
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	54
ДОДАТКИ.....	57
ДОДАТОК А Скрипт ініціалізації середовища РАМ (Privileged Access Management).....	57
ДОДАТОК Б Лістинг програмного коду автоматизації налаштування правомочностей політик Privileged Identity Management.....	59
ДОДАТОК В JSON-конфігурація політики Conditional Access для превентивного захисту.....	60

ВСТУП

Актуальність теми дослідження: Сучасний етап розвитку інформаційних технологій характеризується масовим переходом корпоративних інфраструктур до хмарних сервісів, серед яких екосистема Microsoft 365 посідає лідируючі позиції. Проте концентрація критичних бізнес-даних та інструментів управління в хмарі створює нові вектори атак. Згідно зі статистикою інцидентів кібербезпеки, компрометація привілейованих облікових записів є однією з найнебезпечніших загроз, оскільки надає зловмисникам необмежений контроль над ресурсами компанії.

Традиційні методи захисту, що базуються на постійних адміністративних правах, більше не відповідають вимогам безпеки. Концепція нульової довіри вимагає переходу до динамічного управління доступом. Саме тому впровадження систем Privileged Access Management (PAM), зокрема інструментів Microsoft Entra Privileged Identity Management (PIM), є критично необхідним для забезпечення цілісності та конфіденційності даних у сучасних організаціях.

Об'єкт дослідження - процеси забезпечення інформаційної безпеки в хмарних інфраструктурах та системи управління ідентифікацією.

Предмет дослідження - методи управління привілейованим доступом у середовищі Microsoft 365.

Мета роботи - Захист інформаційних ресурсів корпоративної інфраструктури за рахунок розробки модуля управління привілейованим доступом.

Для досягнення мети було поставлено такі завдання:

1. Аналіз хмарних технологій, можливості інструментів Microsoft Entra ID для захисту ідентифікації.
2. Дослідити розмежування прав доступу на основі принципу найменших привілей (*Least Privilege*).
3. Налаштувати системи доступу при моніторингу та сповіщенню про підозрілу активність адміністраторів.

4. Розробка, налаштування та тестування системи доступу впровадженого рішення захисту інформаційних ресурсів методом найменших привілеїв.

Методи дослідження. У роботі використано методи системного аналізу, моделювання загроз (STRIDE), а також практичні методи конфігурування хмарних систем захисту та автоматизації за допомогою PowerShell.

Практична цінність полягає в розробці і впровадженні адаптивної моделі управління доступом методом найменших привілеїв для зниження ступеня ризиків для інформаційних систем за рахунок мінімізації часу існування активних адміністративних привілеїв до 0 в стані спокою.

РОЗДІЛ 1

АНАЛІЗ ЗАГРОЗ ТА КОНЦЕПЦІЙ УПРАВЛІННЯ ДОСТУПОМ У ХМАРНИХ СЕРЕДОВИЩАХ

1.1 Класифікація загроз обліковим записам у хмарі

У сучасному світі кіберзагроз хмарна інфраструктура Microsoft 365 розглядається як динамічне середовище, де традиційні методи захисту інформації втрачають свою ефективність [1]. Основним об'єктом захисту є ідентифікація користувача, а привілейовані облікові записи адміністраторів перетворюються на найуразливішу та водночас найдорожчу точку входу для зловмисників. Вразливість хмарних сервісів виникає з того, що консолі управління адміністративною мережею доступні через загальнодоступну мережу, що дозволяє атакувати їх віддалено, минаючи фізичні межі компанії [2, 3].

Класифікацію загроз у хмарі можна почати з методів компрометації облікових даних, серед яких найнебезпечнішими є атаки нового покоління, такі як Adversary-in-the-Middle (AiTM) [4]. На відміну від фішингу, AiTM використовує проксі-сервери для перехоплення не тільки паролів, а й токенів сеансу в режимі реального часу. Це дозволяє зловмисникам обійти навіть налаштовану багатофакторну автентифікацію і викрадати вже підтверджений робочий сеанс, після чого вони створюють підтверджений робочий сеанс у своєму середовищі (рис. 1.1) [5].

Поряд з цим активно використовується “Розпилення паролів” (Password Spraying), за допомогою чого зловмисник намагається підібрати один розширений пароль для великої кількості облікових записів одночасно, уникаючи блокування за багаторазові спроби входу для конкретного користувача. Крім того, слід виділити таку вразливість як “втома MFA” (MFA Fatigue). Ця атака базується на психологічній маніпуляції: після крадіжки пароля зловмисник ініціює десятки запитів на підтвердження входу в мобільний додаток адміністратора [5]. В умовах високого навантаження користувач може

випадково або навмисно підтвердити запит на зупинку потоку сповіщень, що надає хакеру повний доступ до системи.

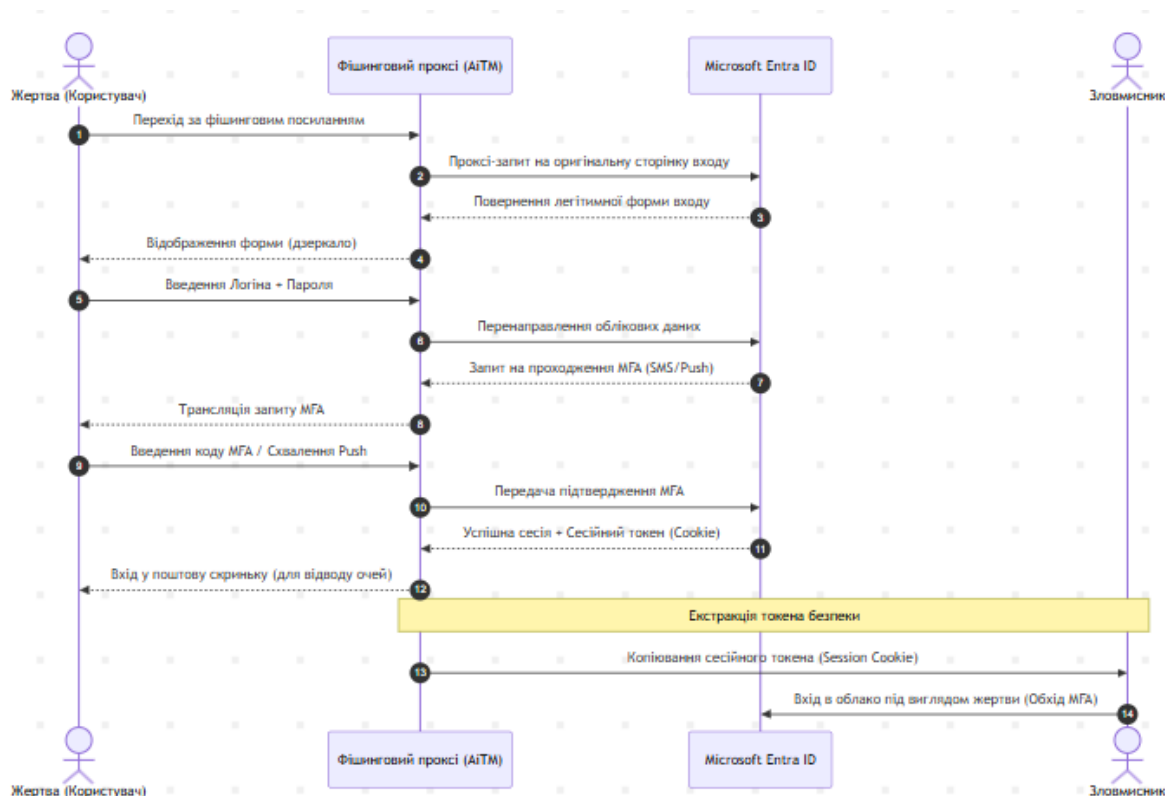


Рисунок 1.1 - Архітектура перехоплення сесії та обходу багатофакторної автентифікації за допомогою Adversary-in-the-Middle.

Особливе місце в ієрархії загроз відведено компрометації через сторонні додатки (OAuth Consent Phishing). Якщо адміністратор з постійними правами надає шкідливому додатку дозвіл через Graph API, зловмисник отримає постійний доступ до даних, незалежно від зміни паролів користувачів (рис. 1.2) [6].

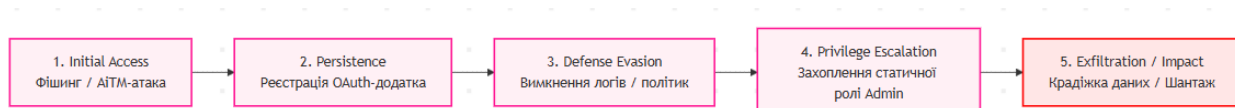


Рисунок 1.2 - Етапи розвитку цілеспрямованої атаки у хмарному середовищі за допомогою Cloud Kill Chain.

Для статистичного аналізу цих ризиків можна використовувати модель STRIDE, яка дозволяє визначити найкритичніші напрямки для Microsoft 365

такі як: Spoofing, Tampering та Elevation of Privilege [7]. Матриця MITRE ATT&CK деталізує ці загрози, таблиця 1.1, за допомогою специфічних технологій, таких як T1098 (маніпуляція обліковими записами) та T1550.004 (вибір ідентифікаційного маркера), що підтверджує їхній статус чітко задокументованих реальних хакерських груп [8].

Таблиця 1.1 - Класифікація критичних загроз середовища M365 за методологією STRIDE та MITRE ATT&CK

Категорія за STRIDE	Конкретна загроза для M365 / Entra ID	Потенційні наслідки для інфраструктури	Техніка MITRE ATT&CK
Spoofing (Підміна)	Видавання себе за адміністратора через викрадений токен або успішну AiTM-атаку.	Повний несанкціонований контроль над хмарним середовищем від імені довіреної особи.	T1550.004 (Use Alternative Authentication Material)
Tampering (Втручання)	Зміна політик Conditional Access, вимкнення засобів захисту чи налаштувань логування.	Створення прихованих “вразливостей” та персистентних бекдорів у системі безпеки компанії.	T1098 (Account Manipulation)
Elevation of Privilege (Підвищення прав)	Несанкційоноване отримання або активація ролі Global Admin за відсутності динамічного контролю.	Найвищий рівень ризику; захоплення контролю над усіма цифровими активами підприємства.	T1548 (Abuse Elevation Control Mechanism)

Джерело: Розроблене автором

Актуальність захисту підтверджується статистикою. Згідно з звітом Microsoft Digital Defense Report 2025, фахівці щодня аналізують понад 38 мільйонів сигналів, пов’язаних з ризиками ідентифікації [9]. Аналіз витрат у звіті IBM Cost of a Data Breach Report 2025 показує, що середня вартість витоку даних через скомпрометовані облікові записи становить приблизно 4,67 мільйона доларів [10]. Цей інцидент, пов’язаний з інсайдерами, оцінюється в середньому в 4,92 мільйона доларів.

Найголовнішою архітектурною загрозою залишається наявність постійних привілеїв [11]. Ситуація, коли адміністратор має високі права цілодобово, створює надмірну поверхню для атаки. У гібридних середовищах це доповнюється ризиком горизонтального переміщення між локальною

службою Active Directory та хмарою. З іншої точки зору, перехід до моделі Just-In-Time (JIT) зменшує поверхню для атаки на 90-95%, при цьому доступ надається лише під час певної операції [12, 13]. Таким чином, аналіз загроз демонструє, що хмарна ідентифікація є багатогранною ціллю, де технічні вразливості переплітаються з методами соціальної інженерії, що вимагає впровадження РАМ системного класу для суворого обмеження та визначення обсягу наданих повноважень.

1.2. Концепція нульової довіри та роль РАМ у її реалізації

У відповідь на складність та диверсифікацію загроз хмарним середовищам, індустрія кібербезпеки перейшла від традиційної моделі “безпечного периметра” до архітектури нульової довіри (ZTA) [14]. Розглядаючи роль РАМ у впровадженні цієї стратегії, необхідно звернути увагу на історичний контекст зміни парадигми безпеки. Протягом десятиліть домінуючою була модель “Замок і рів”, де основна увага приділялася зміцненню зовнішніх меж мережі. Однак з розвитком хмарних обчислень межі корпоративного периметра розмилися і розширилися, що призвело до появи критичної системної помилки: надмірної статичної довіри до сутностей, які вже знаходяться всередині мережі [15].

Основна філософія концепції нульової довіри базується на постулаті: “нікому не довіряй, завжди перевіряй”. Кожен запит на доступ до ресурсів M365 має бути суворо автентифікований та перевірений на основі контекстних сигналів (рис 1.3)

Важливим аспектом є відповідність цієї моделі міжнародним стандартам, таким як NIST SP 800-207, в якому чітко зазначено, що управління привілейованим доступом є одним з основних компонентів архітектури безпеки [16]. Без динамічного управління ідентифікацією неможливо досягти відповідності вимогам стандартів ISO/IEC 27001, SOC2 [17].

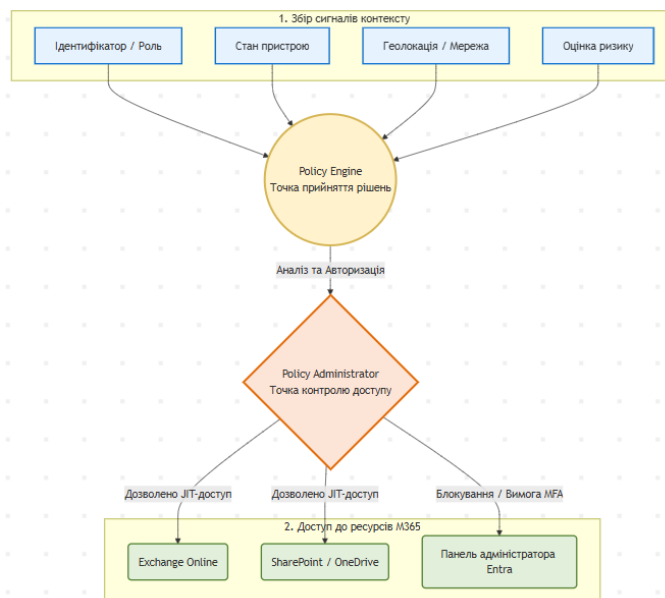


Рисунок 1.3 - Логічна архітектура нульової довіри згідно зі стандартом NIST, де JIT-доступ контролюється через динамічну оцінку сигналів.

Впровадження Zero Trust базується на трьох принципах, де центральну роль відіграють системи PAM, таблиця 1.2.

Таблиця 1.2 - Фундаментальні принципи архітектури Zero Trust та їх практична реалізація за допомогою систем PAM

Принцип Zero Trust	Сутність принципу	Практична реалізація через системи PAM
Verify Explicitly (Явна перевірка)	Аналіз телеметрії перед кожною транзакцією.	Суворі перевірки стану пристрою та примусова багатофакторна автентифікація перед запитом на підвищення привілеїв.
Use Least Privilege (Найменші привілеї)	Надання мінімально необхідних прав на обмежений час.	Механізми JEA для обмеження зони впливу та JIT для обмеження часу активності ролі.
Assume Breach (Припущення зламу)	Проектування мережі з урахуванням того, що інсайдер вже зламаний.	Безперервний моніторинг сесій, сегментація доступу та суворий аудит кожної дії.

Джерело: Розроблене автором

Перший принцип - явна перевірка яка вимагає аналізу телеметрії (стан пристрою, ризик користувача) перед наданням доступу.

Другий принцип - використання найменших привілеїв який реалізується за допомогою механізмів Just-In-Time та Just-Enough-Access [18, 12, 13]. Замість надання постійної ролі, PAM дозволяє активувати права лише на обмежений

період. Ефективність впровадження системи РАМ у межах стратегії ZTA може бути кількісно оцінена через математичне моделювання скорочення вікна вразливості. Нехай T - загальний часовий інтервал (наприклад, тиждень, 168 годин). У звичайній моделі адміністратор має постійні привілеї $t_{\text{static}} = T$. У моделі РАМ з використанням механізму JIT привілеї активуються лише на час виконання завдання t_{active} . Якщо середня тривалість адміністративної сесії становить n годин на день, то сумарний час експозиції за тиждень становить $t_{\text{JIT}} = n \times 7$ а коефіцієнт скорочення ризику K_r можна виразити за формулою 1.1 [14]:

$$K_r = 1 - \frac{t_{\text{JIT}}}{T}, \quad (1.1)$$

При стандартних значеннях ($n = 2$ години на добу), ми отримуємо значення:

$$K_r = 1 - \frac{14}{168} \approx 0.917$$

Це означає, що за рахунок часового обмеження математичне очікування успішної атаки знижується на **91.7%** (рис. 1.4).



Рисунок 1.4 - Порівняння площі вікна атаки між постійними адміністративними привілеями (Standing Privileges) та динамічною активацією Just-In-Time.

Також, впровадження РАМ мінімізує так званий **Blast Radius** (радіус ураження). Якщо при статичних правах злоумисник отримує доступ до 100% ресурсів середовища, то при використанні JEА доступ сегментується. Якщо організація має M типів адміністративних ролей, то доступ надається лише до

1/М частини ресурсів і сумарний показник захищеності (S) можна представити як функцію від часу (t) та обсягу прав (P) згідно з формулою (1.2) [14]:

$$S(t, P) = \frac{1}{e^{t \times P}}, \quad (1.2)$$

Де $t \rightarrow 0$ та $P \rightarrow \min$. Це демонструє експоненціальне зростання складності проведення атаки. У науковій літературі це часто описується як перехід від “об’єктно-орієнтованої” до “транзакційно-орієнтованої” безпеки, де кожна спроба втручання розглядається як окрема транзакція, що потребує індивідуального підтвердження довіри [19].

Третій принцип - припущення зламу, це реалізується через суворий аудит. РАМ перетворює адміністративний доступ із статичного стану на динамічний процес. Крім того, слід враховувати психологічний аспект, сучасні РАМ-рішення в МЗБС проектуються так, щоб забезпечити баланс між безпекою та продуктивністю. Автоматизація робочих процесів схвалення (Approval Workflows) дозволяє реалізувати суворий контроль без значних операційних затримок, формуючи в компанії культуру “свідомої безпеки”, де привілеї розглядаються як відповідальність, що активується виключно для конкретних завдань [20].

1.3. Порівняльний аналіз архітектури РАМ

Ефективність управління привілейованим доступом значною мірою залежить від обраної архітектури рішення, яка повинна повністю відповідати топології, масштабу та специфіці інформаційної системи підприємства [21]. У ході дослідження було проведено детальний порівняльний аналіз двох домінуючих технологічних підходів, що домінують на ринку, а саме традиційних локальних інфраструктурних систем та сучасних хмарних рішень. Цей порівняльний аналіз базується на дослідженні глобальних ринкових тенденцій 2025-2026 років, де хмарні технології остаточно закріпили за собою статус галузевого стандарту для захисту розгалужених SaaS-платформ та розподілених корпоративних ресурсів [22].

Традиційні локальні системи, представлені на ринку рішеннями класу CyberArk або BeyondTrust, будуються на принципі повного посередництва та ізоляції цільових вузлів. Основним архітектурним компонентом такої моделі є Privileged Session Manager (PSM), який виконує роль проксі-сервера, через який примусово маршрутизуються всі адміністративні сесії інфраструктури. Технічна реалізація цього підходу покладається на використання централізованого захищеного сховища облікових даних (Vault), де паролі адміністраторів зберігаються в зашифрованому вигляді та ротуються автоматично за заданим розкладом. У такій парадигмі адміністратор отримує доступ до цільової системи через проксі-вузол, взагалі не знаючи фактичних облікових даних та поточних паролів. Головною технічною перевагою локального підходу є можливість повного відеозапису сесії, ведення детальних текстових логів та розбору мережевих протоколів на рівні окремих введених команд. Проте, при роботі з сучасними хмарними екосистемами, зокрема Microsoft 365, така архітектура створює критичне “пляшкове горло” для трафіку. Весь мережевий потік між хмарним сервісом та робочою станцією адміністратора змушений проходити через локальний дата-центр компанії (ефект hairpinning), що призводить до значних затримок, зниження продуктивності праці ІТ-персоналу та підвищення капітальних витрат на розширення мережевих каналів.

Натомість архітектура хмарних рішень класу Cloud-native PAM, яскравим представником яких є сервіс Microsoft Entra PIM, інтегрована безпосередньо в рівень управління ідентифікацією та автентифікації провайдера послуг [23]. У цій моделі повністю відсутні проксі-сервери або додаткові проміжні вузли, а безперервний контроль здійснюється безпосередньо на рівні зміни стану облікового запису конкретного користувача. Технічна реалізація такої системи динамічно маніпулює членством користувача в адміністративних ролях у режимі реального часу за запитом. Доступ до ресурсів надається не через “видачу пароля” чи компрометацію сховища, а через тимчасове розширення повноважень існуючого облікового запису після успішного проходження всього комплексу превентивних перевірок умовного

доступу [24]. Аналіз такої архітектури свідчить, що вона дозволяє повноцінно використовувати потужну глобальну інфраструктуру сигналів безпеки, включаючи перевірку факторів MFA, оцінку поточного ризику IP-адреси та аналіз стану кінцевого пристрою. Замість ізоляції самої сесії, хмарний PAM фокусується на всебічній перевірці контексту, що є значно ефективнішим, гнучкішим та безпечнішим підходом для динамічних хмарних середовищ [21].

Статистичний та порівняльний аналіз метрик безпеки за період 2025-2026 років чітко демонструє глибоку поляризацію сучасного ринку систем захисту. Згідно з масштабними дослідженнями аналітичних агенцій Gartner та IDC, компанії, які впроваджують саме Cloud-native PAM рішення, демонструють у середньому на 60% швидшу реакцію на виникнення інцидентів та аномальну активність. Це досягається завдяки нативності архітектури та безшовній інтеграції з хмарними системами моніторингу і SIEM-платформами [21, 25]. Зведені результати порівняння техніко-економічних та архітектурних параметрів обох моделей наведені у таблиці 1.3.

Таблиця 1.3 - Порівняльний аналіз техніко-економічних параметрів локальних (On-premise) та хмарних (Cloud-native) архітектур PAM

Параметр порівняння	Традиційний (On-premise)	Хмарний (Cloud-native)
Принцип захисту	Ізоляція сесії та приховування паролів	Динамічне управління ролями та контекстом
Вплив на інфраструктуру	Потребує підтримки серверів та БД	Не потребує локальних ресурсів
Масштабованість	Вертикальна (залежить від “заліза”)	Горизонтальна (автоматична в хмарі)
Середній час впровадження	3-9 місяців	2-6 тижнів
Економічна модель	Капітальні витрати (CapEx)	Операційні витрати (OpEx / Subscription)

Джерело: розроблено автором

Перевагу хмарної архітектури над локальною можна довести математично, порівнявши їхні інтегральні показники ймовірності відмови

(P_f). Оскільки у традиційній локальній інфраструктурі всі компоненти з'єднані послідовно, працездатність системи є критично залежною від безвідмовної роботи кожного її вузла. Ймовірність відмови для такої архітектури виражається формулою 1.3 [13]:

$$P_f = 1 - \prod_{i=1}^n (1 - p_i), \quad (1.3)$$

де n - кількість компонентів (сервери, сховища, мережа), а p_i - ймовірність відмови окремого компонента [19]. У хмарній архітектурі більшість цих компонентів абстраговані та мають рівень доступності (SLA) понад 99.99%, що робить загальну відмову системи статистично менш імовірною. Економічний аналіз (TCO) показує, що за 5-річний період хмарні рішення є на 35-45% вигіднішими завдяки відсутності витрат на оновлення обладнання та утримання штату вузькоспеціалізованих спеціалістів для підтримки РАМ-інфраструктури [26]. Так, для захисту екосистеми Microsoft 365 традиційні архітектури стають “надлишковими” та створюють додаткові ризики безпеки, тоді як хмарний підхід забезпечує органічну інтеграцію та максимальну швидкість захисту привілейованих операцій [27].

1.4. Обґрунтування вибору Microsoft 365 як платформи захисту

Завершальним етапом аналітичного дослідження буде обґрунтування вибору технологічної можливості Microsoft 365 для реалізації системи управління привілейованим доступом. Цей вибір не є випадковим і він базується на комплексному аналізі технічної сумісності, економічної доцільності та стратегічних перевагах інтегрованої системи безпеки [1]. В умовах, коли підприємство вже використовує хмарні сервіси, впровадження стороннього РАМ-рішення створює штучні бар'єри, тоді як вбудовані інструменти забезпечують безшовний захист.

Основним технічним аргументом на користь M365 є архітектурна синергія між Microsoft Entra ID (колишній Azure AD) та сервісом Privileged

Identity Management [23, 28]. На відміну від сторонніх рішень, PIM має прямий доступ до метаданих ідентифікації та може маніпулювати членством у ролях без затримок на реплікацію даних. Це дозволяє реалізувати механізм JIT на рівні ядра системи, що гарантує миттєве відкликання прав після завершення часового ліміту [12]. Крім того, вибір даної платформи надає доступ до потужного інструменту умовного доступу, який виступає в ролі інтелектуального “вартового”, аналізуючи кожен запит на активацію ролі за допомогою алгоритмів машинного навчання (рис. 1.5) [24].

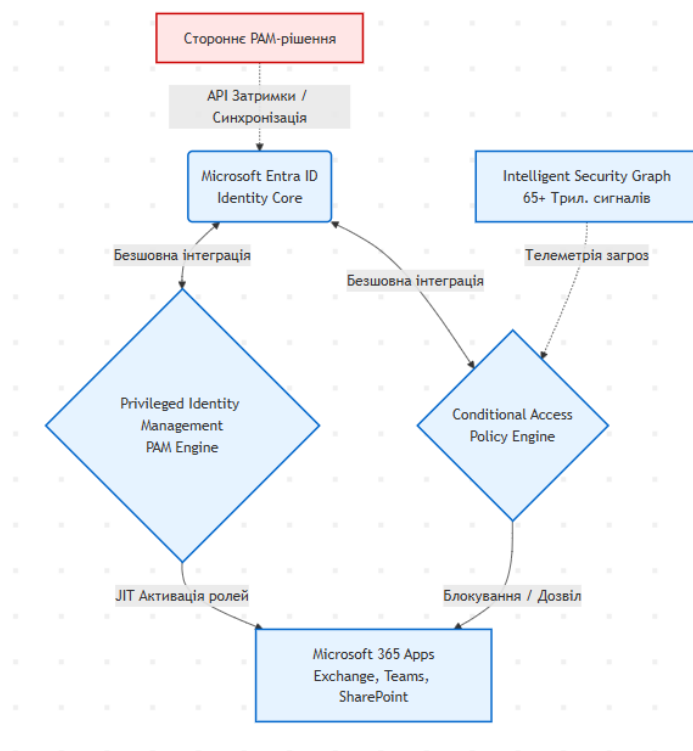


Рисунок 1.5 - Архітектурна синергія вбудованих компонентів Microsoft 365 порівняно з інтеграційними бар'єрами сторонніх PAM-рішень

Згідно до статистично вибіру Microsoft 365 обґрунтовується масштабом глобальної телеметрії Microsoft Intelligent Security Graph. Платформа щомісяця аналізує понад 65 трильйонів сигналів про загрози [9]. Жодне локальне або вузькоспеціалізоване PAM-рішення не володіє такому масивом даних для виявлення аномальної поведінки облікових записів [21]. Таким чином, вибираючи Microsoft 365, ми отримуємо не просто інструмент управління ролями, а глобальну систему раннього попередження про загрози.

З економічного боку це також відіграє вирішальну роль. Використання вбудованого функціоналу Microsoft 365 (за наявності відповідних ліцензій, таких як E5 або Microsoft Entra ID P2) дозволяє уникнути додаткових витрат на закупівлю стороннього ПЗ, що за даними на 2026 рік може заощаджувати компанії до 20%-30% бюджету на безпеку [26]. Це підтверджує раціональність обраного шляху з точки зору оптимізації операційних витрат, таблиця 1.4.

Таблиця 1.4 - Порівняльний аналіз вбудованих рішень архітектури Microsoft 365 та сторонніх РАМ-рішень

Критерій оцінки	Нативне рішення (Microsoft Entra PIM)	Стороннє РАМ-рішення
Архітектурна інтеграція	Безшовна, працює на рівні ядра каталогу.	Потребує API-шлюзів та постійної синхронізації баз даних.
Аналітика загроз	Глобальна (Microsoft Intelligent Security Graph).	Локальна (обмежена даними конкретного підприємства).
Економічна ефективність	Оптимізація OpEx (використання існуючих ліцензій E5/P2).	Високі витрати на закупівлю, розгортання та підтримку.
Час відкликання прав	Миттєво (Continuous Access Evaluation).	Залежить від циклу реплікації стороннього агента.

Джерело: Розроблене автором

Вибір даної платформи максимізує коефіцієнт захищеності (S_c), який можна представити як суму інтегрованих модулів захисту (M_i) за формулою 1.4 [15]:

$$S_c = \sum_{i=1}^k M_i + I_{syn}, \quad (1.4)$$

де I_{syn} - синергетичний ефект від інтеграції. У випадку сторонніх рішень цей ефект часто є від'ємним через складність стикування API, тоді як у Microsoft 365 він є позитивним. Отже, сукупність технічних можливостей, інтеграційного потенціалу та економічної вигоди робить Microsoft 365 оптимальним середовищем для розробки та впровадження системи РАМ.

1.5 Висновки до першого розділу

Дослідження концептуальних засад інформаційної безпеки у хмарних екосистемах засвідчило, що глобальна цифровізація докорінно змінила архітектуру кіберзагроз. Традиційні методи захисту мережевого периметра остаточно втратили свою бар'єрну функцію, поступившись місцем ідентифікації користувача як новому, єдиному рубежу оборони. Проведений аналіз доводить, що беззаперечною мішенню сучасних зловмисників стали саме привілейовані облікові записи. Використання новітніх векторів атак, таких як Adversary-in-the-Middle (AiTM) та психологічна маніпуляція “втома MFA”, дозволяє хакерам успішно обходити стандартні засоби багатфакторної автентифікації. Застосування методології моделювання загроз STRIDE та матриці MITRE ATT&CK підтвердило, що найвищий рівень ризику для корпоративної інфраструктури несе наявність постійних (статичних) адміністративних привілеїв, які створюють невиправдано велику поверхню для атаки.

Доведено, що ефективна протидія цим викликам вимагає обов'язкового переходу до архітектури нульової довіри (Zero Trust), де фундаментальною складовою є впровадження систем класу Privileged Access Management (PAM). За допомогою математичного моделювання обґрунтовано, що реалізація принципу найменших привілеїв через механізми Just-In-Time (JIT) та Just-Enough-Access (JEA) дозволяє експоненціально знизити ризики та скоротити вікно вразливості понад 90%. Це перетворює адміністративний доступ із постійно відкритого стану на динамічний, суворо контрольований процес, який керується контекстом кожної окремої транзакції.

Порівняльний аналіз архітектурних підходів продемонстрував перевагу хмарних (Cloud-native) рішень над традиційними локальними (On-premise) системами, які виявляються неефективними для захисту SaaS-платформ через створення затримок у мережевому трафіку та високі витрати на утримання. На основі комплексної оцінки технічної сумісності, економічної доцільності оптимізації операційних витрат та можливостей використання масивів

глобальної телеметрії загроз (Intelligent Security Graph), платформи Microsoft 365 визначено як оптимальне середовище для розгортання цільової системи РАМ. Нативна архітектурна синергія між ядром Microsoft Entra ID, сервісом Privileged Identity Management (PIM) та превентивними політиками Conditional Access дозволяє реалізувати безшовний захист ідентифікації. Таким чином, сформовано міцне теоретичне та аналітичне підґрунтя для подальшого технологічного дослідження інструментарію та практичної реалізації розробленої моделі безпеки в наступних розділах кваліфікаційної роботи.

РОЗДІЛ 2

ТЕХНОЛОГІЧНІ ОСНОВИ ТА ІНСТРУМЕНТИ MICROSOFT ENTRA ID ДЛЯ ЗАХИСТУ ДОСТУПУ

2.1. Архітектура Microsoft Entra ID та концептуальна модель RBAC

Архітектурна побудова Microsoft Entra ID є результатом фундаментальної трансформації підходів до управління ідентифікацією в епоху глобальної цифровізації [22]. На відміну від класичних серверних рішень, ця система базується на принципах хмарної багатоорендності (Multi-tenancy). Це означає, що в межах єдиної глобальної інфраструктури Microsoft одночасно співіснують мільйони ізольованих інстансів (орендарів), кожен з яких має власну логічну структуру, набір користувачів та унікальні політики безпеки [23]. Така архітектура забезпечує небачену раніше масштабованість: система здатна обробляти мільярди запитів на автентифікацію щодня, зберігаючи при цьому найвищий рівень відмовостійкості та ізоляції даних.

Важливою відмінністю від локальної екосистеми Active Directory (AD) є повна зміна технологічного стека. Якщо традиційна AD спиралася на “важкі” бінарні протоколи, такі як Kerberos та LDAP, що вимагали прямої видимості контролерів домену та специфічних налаштувань локальної мережі, то Entra ID повністю адаптована під реалії інтернету [1]. Вона базується на відкритих веб-стандартах HTTP/HTTPS та використанні архітектури REST API. Це перетворює ідентифікацію з локального інфраструктурного вузла на глобальний сервіс - Identity as a Service (IDaaS) [22].

Завдяки переходу на веб-протоколи, керування доступом у Microsoft Entra ID відбувається на принципово новому рівні. Замість аналізу мережових пакетів у закритому периметрі, система оперує токенами (Security Tokens) та твердженнями (Claims) [23]. Кожен запит адміністратора на доступ до ресурсів Microsoft 365 супроводжується передачею спеціального об'єкта - JSON Web Token (JWT). Цей токен містить не просто пароль, а набір цифрових “тверджень”: ким є користувач, які привілеї він має на даний момент, та за яких умов цей доступ було надано. Це дозволяє реалізувати гнучку авторизацію, де

рішення про надання прав приймається не на основі того, “звідки” прийшов запит, а на основі того, “що саме” відомо про сесію в реальному часі (рис. 2.1).

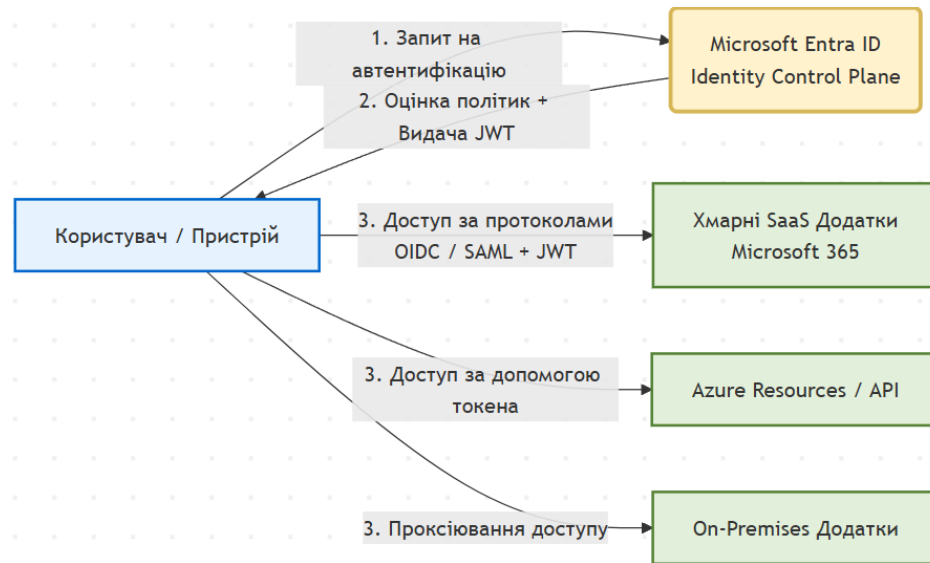


Рисунок 2.1 - Архітектура Identity Control Plane: роль Microsoft Entra ID у видачі JWT-токенів та забезпеченні доступу до розподілених ресурсів.

Аналіз архітектури хмарного середовища вимагає чіткого визначення концепції поверхні атаки (Attack Surface), яка у веб-орієнтованих інфраструктурах зазнає суттєвих трансформацій. У традиційній моделі поверхня атаки обмежувалася фізичними та мережевими кордонами корпоративного периметра, проте в екосистемі IDaaS вона повністю зміщується на рівень цифрової ідентифікації. Поверхня атаки на привілейований доступ у Microsoft 365 визначається сукупністю всіх діючих облікових записів, що володіють адміністративними повноваженнями, кількістю доступних їм атомарних дозволів, а також тривалістю часу, протягом якого ці права залишаються активними. Математично таку залежність площі експозиції ризику можна охарактеризувати як інтегральну функцію від кількості суб'єктів безпеки, обсягу їхніх повноважень та часового чинника. Наявність постійних привілеїв призводить до лінійного розширення цієї поверхні, створюючи ситуацію, за якої зловмисник отримує можливість здійснити несанкціоноване підключення до консолі управління у будь-який момент часу, незалежно від наявності реальної виробничої потреби у виконанні адміністративних завдань. Для превентивного звуження поверхні атаки архітектура Microsoft Entra ID

потребує впровадження інструментів суворого структурного та часового обмеження прав доступу, що лежить в основі сучасних систем захисту інформації.

Логічна модель доступу всередині цієї архітектури реалізується через механізм Role-Based Access Control (RBAC), який спроектований для того, щоб структурувати хаотичний набір індивідуальних прав у зрозумілу ієрархію повноважень [29]. Модель будується на взаємодії трьох ключових архітектурних одиниць, інтегрованих у єдиний захисний контур. Першою одиницею виступають суб'єкти безпеки (Security Principals), які представляють собою цифрові ідентифікатори, що претендують на виконання дій; окрім звичайних користувачів, архітектура підтримує інструменти Service Principals для додатків та Managed Identities для автоматизованих хмарних сервісів, що дозволяє повністю виключити людський фактор із процесів автоматизації. Другою одиницею є визначення ролей (Role Definitions), які діють як інтелектуальні шаблони, що містять перелік атомарних дозволів, завдяки чому замість надання повного доступу архітектура дозволяє створювати ролі з вузькою спеціалізацією, що є практичним втіленням принципу мінімальних привілеїв. Третьою одиницею виступає область дії (Scope), яка є архітектурним обмежувачем, що визначає географію або логічні межі застосування прав, гарантуючи, що навіть при наявності високих привілеїв адміністратор зможе застосувати їх лише до тих об'єктів, які входять до його зони відповідальності. Концептуальний зв'язок цих об'єктів відображено на рисунку 2.2, а практична реалізація принципу найменших привілеїв (Least Privilege) через структурне сегментування повноважень наведена у таблиці 2.1.

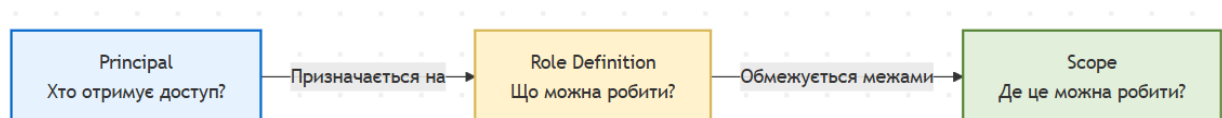


Рисунок 2.2 - Концептуальний зв'язок об'єктів Role-Based Access Control (RBAC) у системі Entra ID.

Таблиця 2.1 - Реалізація принципу найменших привілеїв через механізми структурування ролей та Scope в Entra ID

Компонент моделі	Технічний механізм в Entra ID	Спосіб обмеження поверхні атаки	Ефект для інформаційної безпеки інфраструктури
Суб'єкт (Principal)	Використання Managed Identities для системних служб.	Вилучення статичних паролів та облікових даних із коду додатків.	Повне виключення ризику витоку адміністративних паролів через людський фактор [1].
Роль (Role Definition)	Заміна вбудованої ролі Global Admin на Custom Roles.	Надання виключно атомарних дозволів (наприклад, тільки microsoft.directory/users/password/update).	Обмеження функціональних можливостей адміністратора чіткими межами завдання [13].
Область дії (Scope)	Застосування адміністративних одиниць (Administrative Units).	Обмеження географії дії ролі конкретним департаментом або регіональною філією.	Запобігання горизонтальному переміщенню хакера (Lateral Movement) у масштабах всього тенента [30].

Джерело: Розроблене автором

Математична формалізація архітектурної моделі RBAC

Нехай архітектура системи описується теоретико-множинною моделлю, побудованою відповідно до загальних методів формалізації розширених систем рольового контролю доступу (2.1) [19]:

$$M = (U, R, P, S, App), \quad (2.1)$$

де:

- $U = \{u_1, u_2, \dots, u_n\}$ - множина унікальних суб'єктів (користувачів або сервісних ідентифікаторів);
- $R = \{r_1, r_2, \dots, r_m\}$ - множина адміністративних ролей;

- $P = \{p_1, p_2, \dots, p_k\}$ - множина атомарних **дозволів** (permissions) на виконання операцій;
- $S = \{s_{global}, s_{aul}, \dots, s_{aun}\}$ - ієрархічна множина **областей дії** (scopes);
- $App: = U \times R \times S \rightarrow \{0,1\}$ - предикат призначення, що визначає стан доступу.

В межах цієї моделі, кожна роль $r_i \subseteq P$ визначається як непуста підмножина дозволів:

Процес надання доступу в стандартній моделі RBAC є статичним відображенням. Проте, архітектура Entra ID впроваджує **функцію авторизації на основі тверджень (Claims)**. Якщо користувач u запитує доступ до ресурсу в області дії s з роллю r , система генерує токен T_u , який можна представити як набір логічних предикатів, що визначають умови відповідності суб'єктів (2.2) [19]:

$$T_u = \{(r_j, s_l) | App(u, r_j, s_l) = 1\}, \quad (2.2)$$

Головним недоліком такої статичної моделі є відсутність часового параметру, що призводить до існування постійних привілеїв. Для обґрунтування впровадження РАМ ми модифікуємо предикат призначення, вводячи часову складову t та контекстний вектор C згідно з формулою 2.3, що розширює простір станів системи доступу [19]:

$$App_{PAM}(u, r, s, t, C) = 1 \Leftrightarrow (t \in [t_{start}, t_{end}])^{C \in C_{safe}}, \quad (2.3)$$

Де C_{safe} - підмножина безпечних станів (відповідність пристрою, MFA, низький рівень ризику). Така формалізація доводить, що безпека системи в хмарній архітектурі залежить не лише від ієрархії ролей (R), а й від динамічного контролю часового вікна активації.

2.2. Функціональні можливості Privileged Identity Management (PIM)

Впровадження концепції динамічного управління привілеями вимагає наявності розвиненого інструментарію, який здатен трансформувати статичну модель доступу в адаптивну систему. Сервіс Privileged Identity Management (PIM) виступає як інтелектуальна надбудова над ядром Microsoft Entra ID, надаючи функціональні можливості для контролю кожного етапу життєвого циклу адміністративних повноважень [28]. Основа функціоналу PIM полягає у переході від застарілої парадигми “адміністратор за посадою” до “адміністратор за потребою”, що є критично важливим для зменшення ймовірності реалізації внутрішніх та зовнішніх загроз хмарній інфраструктурі підприємства.

Фундаментальною можливістю сервісу PIM є практична реалізація моделі доступу “саме вчасно” (Just-In-Time) [12]. Технологічно це реалізовано через логічне розщеплення класичного поняття “призначення ролі” на два принципово різні стани, а саме правомочний (Eligible) та активний (Active). Стан правомочності дозволяє користувачу бачити роль у своєму переліку доступних привілеїв, проте за замовчуванням не надає жодних фактичних прав у системі. Це “сплячий” стан, який не може бути успішно використаний злоумисником навіть у разі компрометації та крадіжки поточного сесійного токена, оскільки в самому JWT-токені відсутні відповідні адміністративні претензії та маркери доступу [23]. Натомість стан активації - це тимчасовий перехід, що супроводжується генерацією нового токена безпеки з обмеженим терміном дії. Функціонал PIM дозволяє адміністраторам безпеки проектувати гнучкі часові політики (Time-bound policies), де чітко визначається максимальна тривалість активної сесії, яка зазвичай варіюється в діапазоні від тридцяти хвилин до восьми годин. Після завершення цього визначеного терміну система в автоматичному режимі, без залучення людського фактора чи участі оператора, здійснює миттєве та безповоротне відкликання прав на рівні Identity Provider [28, 13].

Для обґрунтування доцільності розгортання динамічного захисту ідентифікаторів необхідно провести глибокий порівняльний аналіз між

класичним статичним призначенням повноважень та інноваційним підходом на основі тимчасової ескалації прав через сервіс PIM. Традиційні статичні конфігурації створюють постійний вектор загрози, оскільки права доступу адміністратора залишаються незмінними 24 години на добу, що підвищує ризики успішного перехоплення сесійних токенів або компрометації облікових даних. На відміну від цього, хмарна архітектура PIM нівелює ризик постійної наявності високих прав, переводячи ідентифікатори у пасивний стан правомочності. Детальна матриця порівняльного аналізу за ключовими параметрами безпеки та операційного контролю наведена у таблиці 2.2.

Таблиця 2.2 - Порівняльний аналіз архітектурних параметрів статичної моделі ролей та динамічної системи Microsoft Entra PIM

Критерій порівняння	Статична модель призначення ролей	Динамічна модель Microsoft Entra PIM
Час життя привілеїв (TTL)	Необмежений (Постійні standing privileges).	Строго лімітований (Від 30 хвилин до 8 годин) [13].
Стан токена безпеки (JWT)	Завжди містить адміністративні претензії ролі.	Містить привілеї виключно у проміжку активної сесії [23].
Контроль накопичення прав	Високий ризик виникнення Privilege Creep.	Автоматичне вилучення через Access Reviews [28].
Захист від витоку пароля	Провалено (Пароль забезпечує миттєвий доступ).	Успішно (Потрібне повторне MFA та схвалення ролі) [20].
Цифровий слід для аудиту	Фіксуються лише дії, виконані під роллю.	Фіксується факт, час, обґрунтування та автор схвалення [28].

Джерело: Розроблене автором

Поряд із цим функціонал PIM забезпечує можливість налаштування складних багатокритеріальних ланцюжків підтвердження запитів, що повністю виключає одноосібний деструктивний вплив на критичні вузли системи та реалізує принцип подвійного контролю [20]. До основних інструментів превентивної валідації належить вимога ділового обґрунтування (Business Justification), яка зобов'язує користувача ввести текстовий опис запланованих робіт або додати пряме посилання на квиток у корпоративній системі технічної підтримки (ITSM), що забезпечує нерозривний зв'язок між технічною дією та адміністративною подозвільністю. Для найбільш ризикованих та критичних

ролей, таких як Глобальний адміністратор, функціонал дозволяє примусово налаштовувати делеговане схвалення (Approval Workflow). У цьому сценарії активація привілеїв стає абсолютно неможливою без цифрового підпису та затвердження з боку призначеної групи схвалювачів (Approvers), які детально аналізують доцільність запиту. Крім того, на відміну від стандартного входу в систему, PIM дозволяє вимагати повторну багатофакторну перевірку (On activation, require MFA) безпосередньо в момент ескалації прав, що ефективно нівелює ризики використання зловмисниками залишених без нагляду розблокованих робочих станцій легітимних співробітників [28].

Одною з найбільш трудомістких задач у великих організаціях є регулярний аудит актуальності раніше наданих прав. Функціональна можливість оглядів доступу (Access Reviews) дозволяє повністю автоматизувати цей процес за заданим розкладом [13]. Система за визначеним розкладом ініціює цикли перевірок, під час яких відповідальні особи, керівники підрозділів або безпосередні власники ресурсів повинні підтвердити необхідність збереження правомочності для кожного адміністратора. З точки зору інформаційної безпеки, цей функціонал успішно вирішує проблему накопичення привілеїв (Privilege Creep), коли співробітник під час зміни посад або переходу в інші відділи зберігає доступ до попередніх інфраструктурних систем. Якщо під час чергового огляду правомочність не підтверджується відповідальною особою, сервіс PIM автоматично видаляє призначення облікового запису, забезпечуючи суворе дотримання принципу найменших привілеїв у довгостроковій перспективі.

Завершальним блоком функціональних можливостей архітектури є підсистема глибокого аудиту та безперервного моніторингу. Сервіс PIM фіксує не лише факт наявності прав у каталозі, а й кожную спробу їх сесійної активації користувачами, включаючи всі відхилені системою запити, текстові обґрунтування та дії призначених апроверів [28]. Ці детальні лог-дані консоліднуються в інтерактивних внутрішніх звітах та можуть автоматично експортуватися до систем класу SIEM, зокрема Microsoft Sentinel, за допомогою нативних діагностичних інструментів [25]. Це дозволяє службі безпеки

використовувати сучасні інструменти поведінкового аналізу для оперативного виявлення прихованих аномалій, таких як нетиповий нічний час активації привілеїв або масові паралельні запити на доступ до чутливих ролей, що може свідчити про підготовку зломисників до проведення цілеспрямованої атаки на хмарну екосистему.

2.3. Політики умовного доступу як інструмент превентивного захисту

У сучасній архітектурі безпеки, що базується на принципах Zero Trust (Нульової довіри), концепція статичного мережевого периметра остаточно поступилася місцем динамічній перевірці кожного запиту [27]. В екосистемі Microsoft Entra ID ключовим механізмом, що реалізує цей підхід, є політики умовного доступу (Conditional Access) [23]. Вони виступають у ролі інтелектуального “фільтра” або точки прийняття рішень (Policy Decision Point), яка аналізує контекст кожної спроби доступу адміністратора до привілейованих ресурсів ще до того, як права будуть активовані [24]. Це дозволяє реалізувати превентивний захист, де доступ не просто надається або забороняється, а адаптується до рівня загрози в реальному часі.

Технологічна суть умовного доступу полягає в агрегації та обробці масиву сигналів, що надходять від користувача, пристрою, мережі та додатків [23]. На відміну від традиційних систем, де доступ надається виключно на основі знання пароля, превентивний захист у Microsoft 365 комплексно оцінює сукупність факторів, що формують цілісну картину безпеки сесії. Під час цього процесу система здійснює детальний аналіз географічного розташування та мережевого контексту, вивчаючи поточну IP-адресу на предмет її приналежності до анонімних мереж (Tor, VPN-проксі) або країн, що не входять до списку дозволених для конкретної компанії. Паралельно, за допомогою глибокої інтеграції з системою Microsoft Intune, політики умовного доступу перевіряють стан та відповідність пристрою (Device Compliance), контролюючи, чи є пристрій адміністратора корпоративним, чи встановлені на ньому актуальні оновлення безпеки та чи активоване апаратне шифрування

диска [31]. Важливу роль відіграє аналіз рівня ризику ідентифікатора (Identity Risk), де використання алгоритмів машинного навчання дозволяє вчасно виявляти аномалії, такі як “неможливе переміщення” (Impossible Travel) або спроби входу з використанням скомпрометованих облікових даних, що були виявлені у відкритих базах витоків (рис. 2.3) [24].

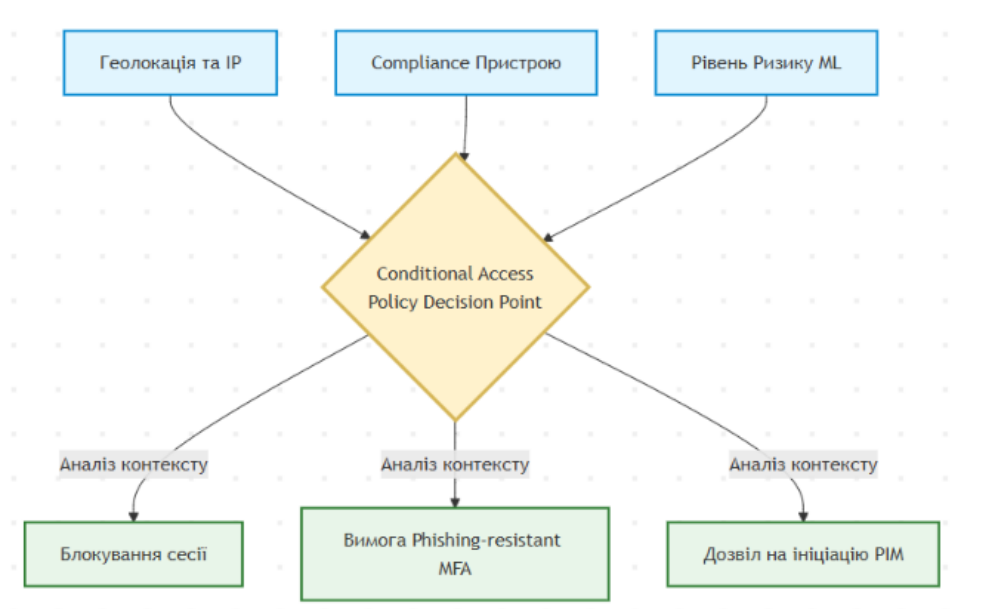


Рисунок 2.3 - Логіка обробки сигналів контексту точкою прийняття рішень (PDP) у системі Conditional Access.

Завдяки такій багатофакторній перевірці умовний доступ створює динамічний захисний бар'єр. Якщо хоча б один із аналізованих параметрів телеметрії не відповідає встановленим критеріям безпеки, система автоматично коригує вимоги до автентифікації або повністю блокує транзакцію. Це дозволяє нівелювати загрози, пов'язані з використанням викрадених сесійних токенів, оскільки спроба отримати доступ до консолі управління з невідомого або невідповідного пристрою буде припинена на ранній стадії, забезпечуючи надійну ізоляцію хмарних активів підприємства [24, 32].

2.4. Методи автентифікації та захисту від компрометації облікових даних

Ефективність функціонування будь-якої системи управління привілейованим доступом критично залежить від надійності механізмів

автентифікації, які виступають першим і найважливішим ешеленом оборони. В умовах сучасної хмарної інфраструктури традиційний захист за допомогою паролів втратив свою актуальність через стрімкий розвиток методів соціальної інженерії, фішингу та атак типу “brute-force” [5]. Для захисту адміністративних облікових записів, які володіють найвищим рівнем повноважень у Microsoft 365, проектування системи автентифікації має базуватися на принципах стійкості до компрометації та використанні багатофакторних моделей перевірки.

Основним інструментом у цьому контексті є багатофакторна автентифікація (MFA), яка в екосистемі Microsoft Entra ID реалізована як динамічний процес підтвердження особи [23]. Технологічно MFA базується на комбінації незалежних факторів: знання (пароль), володіння (фізичний пристрій або апаратний ключ) та приналежність (біометричні дані). Проте для адміністраторів критично важливо використовувати методи, що мають імунітет до перехоплення сесії. Одним із таких методів є Windows Hello for Business, який замінює паролі парою асиметричних криптографічних ключів [33]. Закритий ключ надійно зберігається в апаратному модулі TPM (Trusted Platform Module) робочої станції адміністратора і ніколи не залишає пристрій. Це означає, що зломисник не зможе викрасти облікові дані дистанційно, оскільки автентифікація жорстко прив’язана до конкретного “заліза” та активується лише після біометричного підтвердження (відбиток пальця або сканування обличчя).

Обґрунтувати надійність багатофакторного підходу можна через модель оцінки ймовірності успішної атаки. Нехай $P(f_1)$ - ймовірність зламу першого фактора (наприклад, через фішинг пароля), а $P(f_2)$ - ймовірність компрометації другого фактора (наприклад, викрадення фізичного FIDO2-ключа). За умови повної незалежності цих факторів, загальна ймовірність компрометації системи $P(C)$ обчислюється як їхній добуток за формулою (2.4) [15]:

$$P(C) = P(f_1) \cdot P(f_2), \quad (2.4)$$

Оскільки значення ймовірностей для кожного фактора є малими величинами (наприклад, 10^{-4} та 10^{-7} , їх добуток дає екстремально низький показник ризику, що на практиці означає майже повну захищеність від автоматизованих атак. Це математично підтверджує, що впровадження другого фактора підвищує захищеність не просто вдвічі, а на кілька порядків.

Окремої уваги заслуговує захист від новітніх методів атак, таких як MFA Fatigue (втома від MFA) та Adversary-in-the-Middle (AiTM) [4, 5]. Для протидії “втомі від сповіщень”, коли користувач випадково схвалює запит на вхід через масові Push-повідомлення від зловмисника, у Microsoft Entra ID впроваджено функцію Number Matching (зіставлення чисел) [23]. Користувач повинен ввести на своєму мобільному пристрої саме те число, яке відображається на екрані входу, що гарантує його фізичну присутність перед монітором та усвідомленість дії. Для захисту від складніших AiTM-атак, де зловмисник проксіює трафік і викрадає сесійні токени, проєктована система спирається на стандарти FIDO2 (Fast Identity Online) [34]. Ключі FIDO2 використовують доменне ім'я ресурсу при генерації підпису, тому спроба автентифікації на фішинговому сайті з іншою адресою автоматично зазнає невдачі на рівні протоколу, оскільки підпис не буде валідним для оригінального ресурсу Microsoft [33].

Завершальним етапом захисту є перехід до стратегії Passwordless (безпарольного доступу) [35]. Вилучення пароля як такого з процесу автентифікації повністю ліквідує цілий клас загроз, пов'язаних із підбором, крадіжкою або повторним використанням паролів. Використання Passkeys та сертифікатів дозволяє перетворити обліковий запис адміністратора на цифровий сейф, доступ до якого можливий лише за наявності довіреного пристрою та успішної біометричної перевірки. Така багаторівнева модель, де автентифікація інтегрована з аналізом ризиків умовного доступу, створює максимально надійне середовище для подальшої активації привілейованих ролей через систему PIM, забезпечуючи цілісність та конфіденційність адміністративних операцій у хмарі [28, 24].

2.5 Висновки до другого розділу

Аналіз технологічного базису Microsoft Entra ID засвідчив, що еволюція корпоративних інфраструктур вимагає принципової відмови від застарілих локальних протоколів на користь хмарно-орієнтованої парадигми Identity as a Service (IDaaS). Сучасне керування доступом на рівні Identity Control Plane спирається на використання маркерів безпеки JSON Web Token (JWT) та динамічні твердження (Claims), що дозволяє оцінювати контекст кожної сесії в реальному часі. Проте проведена теоретико-множинна формалізація класичної моделі ролевого розмежування прав (RBAC) довела її критичну вразливість - відсутність часового виміру призначення, що неминуче призводить до існування небезпечних постійних привілеїв, які виступають головною ціллю для зловмисників.

Вирішенням цієї фундаментальної архітектурної проблеми є інтелектуальний сервіс Privileged Identity Management (PIM), який трансформує статичну безпеку в адаптивну модель доступу "саме вчасно" (Just-In-Time). Завдяки технологічному розподілу повноважень на стани правомочності (Eligible) та тимчасової сесійної активації (Active), система зводить площу потенційної атаки до мінімуму. Впровадження інструментів багатокритеріальної валідації запитів, обов'язкового надання ділового обґрунтування, делегованих процесів багатокрокового схвалення (Approval Workflows) та автоматизованих оглядів доступу (Access Reviews) ефективно ліквідує загрозу накопичення привілеїв (Privilege Creep) і формує надійний, прозорий цифровий слід для систем аналітики та аудиту.

Невід'ємною складовою побудови превентивного захисту адміністративних ідентифікаторів є політики умовного доступу (Conditional Access), які виконують функцію точки прийняття рішень (Policy Decision Point). Глибока інтеграція цих політик із модулями управління кінцевими точками Microsoft Intune та алгоритмами машинного навчання Entra ID Protection дозволяє системі безперервно агрегувати сигнали середовища. Оцінка мережевої геолокації, перевірка відповідності пристрою жорстким критеріям

безпеки (Device Compliance) та аналіз поведінкового ризику сесії гарантують блокування несанкціонованих запитів ще до моменту ініціації ескалації прав.

Фундаментом стійкості цієї ешелонованої оборони виступають криптографічно надійні методи перевірки особи. Математично доведено, що багатофакторні моделі автентифікації експоненціально знижують ймовірність компрометації системи. Використання апаратних ключів FIDO2, технології Windows Hello for Business з апаратною ізоляцією закритих ключів у модулях TPM, а також активна протидія “втомі MFA” через функцію зіставлення чисел (Number Matching) гарантує імунітет системи проти фішингових атак нового покоління (AiTM). Отже, детальний аналіз підтверджує, що інструментарій Microsoft Entra ID формує повноцінну, технічно довершену екосистему для реалізації принципів нульової довіри (Zero Trust), створюючи міцне аналітичне підґрунтя для переходу до етапу практичного налаштування системи.

РОЗДІЛ 3

ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ РАМ У СЕРИДОВИЩІ ПІДПРИЄМСТВА

3.1. Підготовка хмарної інфраструктури та базове налаштування середовища

Для практичної реалізації та дослідження розробленої системи керування привілейованим доступом (РАМ) необхідно підготувати ізольоване хмарне середовище. Використання ізольованого тестового орендаря (Tenant) дозволяє проводити експерименти з критичними політиками безпеки без ризику порушення бізнес-процесів операційної компанії. Технологічною основою для розгортання системи є інфраструктура Microsoft Entra ID, яка вимагає попереднього налаштування основних параметрів та забезпечення відповідних ліцензійних передумов.

Першим кроком у підготовці середовища є забезпечення відповідного рівня ліцензування. Базова функціональність Microsoft Entra ID (безкоштовні або базові плани Microsoft 365) підтримує лише статичну модель RBAC, яку ми визнали вразливою. Щоб розблокувати динамічні механізми, необхідно активувати ліцензію Microsoft Entra ID Premium P2. Цей рівень ліцензування є критично важливим, оскільки він забезпечує доступ до трьох ключових компонентів нашої системи:

- Керування привілейованими ідентифікаторами (PIM): для налаштування процесів доступу та затвердження Just-In-Time.
- Захист Microsoft Entra ID: для генерації сигналів ризику користувача та ризику входу на основі машинного навчання.
- Розширений умовний доступ: для можливості створення політик, що маршрутизують запити на основі сигналів ризику.

Після реєстрації тестового клієнта (наприклад, у доменній зоні .onmicrosoft.com) активується пробний період Premium P2, що дозволяє повністю розгорнути архітектуру без додаткових фінансових витрат на етапі дослідження.

Наступним етапом практичної підготовки є створення логічної структури, яка буде імітувати реальне корпоративне середовище. Для чистого експерименту необхідно відмовитися від практики використання єдиного глобального адміністратора та змодельовати ієрархію, описану в нашій моделі рівняння.

Процес налаштування включає такі технічні кроки:

- Створення цільових облікових записів (ідентифікацій): У базі даних каталогу створюються тестові користувачі. Для чистоти експерименту створюються як звичайні користувачі (без будь-яких прав), так і користувачі, які в майбутньому отримають статус привілейованого. На цьому етапі генеруються надійні початкові паролі для всіх адміністративних облікових записів та ініціюється процес примусової реєстрації методів MFA (наприклад, Microsoft Authenticator).
- Формування груп безпеки (Security Groups): Замість призначення ролей безпосередньо кожному користувачеві створюються спеціалізовані групи безпеки (наприклад, SG-Exchange-Admins, SG-Helpdesk). Microsoft Entra ID надає можливість створювати так звані Role-assignable groups (групи, яким можна призначати ролі). Це дозволяє керувати привілеями на рівні групи: щойно користувач додається до групи, система PIM автоматично застосовує до нього відповідні політики доступу.
- Налаштування адміністративних одиниць (Administrative Units): Для моделювання великої компанії з регіональними філіями створюються адміністративні одиниці. Наприклад, створюється AU. Це робиться для того, щоб продемонструвати концепцію Scope під час експерименту, коли адміністратор підтримки матиме право скидати паролі лише для користувачів з цієї філії, не маючи доступу до управління організацією.

Перед активацією інтелектуальних систем PIM та умовного доступу необхідно усунути базові вразливості на рівні протоколу. Найбільшою загрозою для будь-якого хмарного середовища є використання застарілих протоколів автентифікації (Legacy Authentication), таких як POP3, IMAP або SMTP. Ці протоколи технічно не підтримують передачу токенів

багатофакторної автентифікації. Якщо їх не вимкнути, зломисник зможе обійти всі наші складні політики умовного доступу, просто надіславши базовий запит із викраденим логіном та паролем через застарілий поштовий клієнт.

Щоб закрити цей вектор атаки на рівні клієнта, активується політика Security Defaults (або створюється відповідне глобальне правило умовного доступу), яка жорстко блокує будь-які запити, що не підтримують сучасну автентифікацію.

Завершення цього етапу означає, що хмарна інфраструктура очищена від застарілих вразливостей, розділена на логічні сегменти та повністю готова до розгортання інтелектуальних політик підвищення привілеїв.

“Для забезпечення стандартизації та уникнення людських помилок під час розгортання базової інфраструктури було розроблено скрипт автоматизації на базі Microsoft Graph PowerShell. Повний лістинг програмного коду, який формує ієрархію привілейованих груп (Role-assignable groups) та створює ізольовані адміністративні одиниці, наведено у Додатку А (рис. 3.1).”

```
# 1. Авторизація в Microsoft Entra ID з необхідними правами
Connect-MgGraph -Scopes "Group.ReadWrite.All", "AdministrativeUnit.ReadWrite.All",
"Directory.ReadWrite.All"

Write-Host "З'єднання встановлено. Початок розгортання структури..." -
ForegroundColor Green

# 2. Створення Адміністративних одиниць (Administrative Units) для сегментації
$auName = "Kyiv_Branch_AU"
$auDescription = "Адміністративна одиниця для ізоляції ресурсів Київського офісу"

$newAu = New-MgAdministrativeUnit -DisplayName $auName -Description $auDescription
Write-Host "Створено Administrative Unit: $($newAu.DisplayName)" -ForegroundColor
Cyan
```

Рисунок 3.1 - Скрипт ініціалізації середовища PAM (Privileged Access Management)

Даний скрипт використовується для первинної підготовки хмарного середовища Microsoft Entra ID. Він автоматизує створення Адміністративних одиниць (Administrative Units) для логічної ізоляції ресурсів та формує ієрархію привілейованих груп безпеки (Privileged Access Groups) відповідно до трирівневої моделі (Tier 0, Tier 1, Tier 2).

3.2. Практичне налаштування політик керування привілейованими ідентифікаторами (PIM)

Після успішної підготовки базової хмарної інфраструктури та забезпечення вимог до ліцензування наступним критичним етапом є практичне впровадження механізмів динамічного керування привілеями [23]. Процес налаштування служби керування привілейованими ідентифікаторами (PIM) у панелі керування Microsoft Entra ID вимагає послідовного переходу від застарілої парадигми постійних прав до сучасної моделі доступу “Just-In-Time” (JIT) [28, 12]. Цей етап є центральним для впровадження концепції найменших привілеїв, оскільки саме тут безпосередньо налаштовуються часові, логічні та авторизаційні обмеження для кожної адміністративної ролі [13]. Першим практичним кроком у розгортанні системи є проведення процедури виявлення для існуючих призначень. Система PIM ініціює глибоке сканування каталогу, щоб ідентифікувати всі облікові записи користувачів та принципи служб, які мають постійні активні привілеї [30]. Щоб усунути поверхню атаки, пов’язану з постійними привілеями, виявлені постійні призначення примусово перетворюються адміністратором безпеки у стан “Допустимий” [18]. На практиці це означає, що користувач повністю втрачає свої адміністративні привілеї в стані очікування, але зберігає право ініціювати запит на їх тимчасове отримання [28].

Наступним кроком є детальне налаштування параметрів активації (налаштування ролей) для різних груп привілеїв. Для практичної реалізації моделі багаторівневого доступу політики налаштовуються по-різному залежно від критичності ролі [11]. Ролі найвищого рівня доступу Tier 0 (Глобальний адміністратор, Адміністратор привілейованої ролі, Адміністратор безпеки) мають найсуворіші обмеження. Максимальна тривалість одного активного JIT-сеансу обмежена двома годинами, що гарантує, що навіть у разі компрометації токена сеансу вікно можливостей для зловмисника буде критично малим [13]. Для операційних ролей Tier 1 (Адміністратор Exchange, Адміністратор користувачів), які використовуються інженерами для щоденної підтримки

інфраструктури, вікно активації подовжується до восьми годин, що відповідає стандартному робочому дню. Це дозволяє підтримувати баланс між високим рівнем безпеки та комфортом ІТ-персоналу, таблиця 3.1 [11].

Таблиця 3.1 - Матриця конфігурації політик активації ролей у сервісі Microsoft Entra PIM за рівнями моделі Tiering.

Рівень доступу	Цільова роль / Група в Entra ID	Максимальний час активації	Вимога MFA при активації	Вимога обґрунтування (ITSM-квиток)	Багатокрокове схвалення (Approval Workflow)
Tier 0	Global Administrator	2 години	Так (Phishing-resistant)	Так (Обов'язково)	Так (Група: Security Team)
Tier 0	Privileged Role Administrator	2 години	Так (Phishing-resistant)	Так (Обов'язково)	Так (Група: Security Team)
Tier 0	Security Administrator	4 години	Так (Phishing-resistant)	Так (Обов'язково)	Так (Група: CISO/Lead SecOps)
Tier 1	Exchange Administrator	8 годин	Так	Так (Обов'язково)	Ні (Автоматична активація)
Tier 1	Intune Administrator	8 годин	Так	Так (Обов'язково)	Ні (Автоматична активація)
Tier 1	SharePoint Administrator	8 годин	Так	Так (Обов'язково)	Ні (Автоматична активація)
Tier 2	Helpdesk Administrator	8 годин	Так	Так (Обов'язково)	Ні (Автоматична активація)
Tier 2	User Administrator (Обмежено AU)*	8 годин	Так	Так (Обов'язково)	Ні (Автоматична активація)

Джерело: Розроблене автором

Незалежно від рівня ролі, налаштування PIM автоматично активують вимогу повторного проходження багатфакторної автентифікації безпосередньо під час ескалації прав (On activation, require MFA) [33]. Цей крок є обов'язковим, оскільки підтверджує фізичну присутність легітимного користувача перед пристроєм саме в момент ініціювання критичної дії [23]. Додатково вводиться вимога надання бізнес-обґрунтування (Require justification). Практичне налаштування зобов'язує адміністратора вводити не

лише текстовий опис причини доступу в спеціальне поле, але й номер відповідного інциденту або запиту на зміну від корпоративної системи управління IT-послугами (ITSM / Service Desk) [28]. Це створює надійний цифровий слід для подальшого аудиту [20]. Для найбільш критичних дозволів система додатково налаштовує багатоетапний процес затвердження (Approval Workflow) [20]. Налаштування цієї політики передбачає блокування автоматичної видачі дозволів навіть після успішної MFA та введення обґрунтування. Натомість запит переводиться в стан очікування (Pending) та направляється до певної групи затверджувачів (Approvers). Тільки після того, як уповноважена особа проаналізує запит та натисне кнопку затвердження у своєму інтерфейсі PIM, система генерує токен з новими дозволами для ініціатора [28, 20]. Цей механізм практично реалізує класичний принцип безпеки “подвійного контролю” (принцип чотирьох очей).

Окрім класичних ролей Entra ID, на цьому етапі також налаштовується функціональність PIM for Groups [30]. До системи управління підключаються створені на попередньому етапі привілейовані групи безпеки (Privileged Access Groups). Це дозволяє масштабувати архітектуру в майбутньому: користувачі запитуватимуть активацію не конкретних хмарних ролей, а членства у відповідній групі, яка вже може містити набір прав доступу до різних сервісів, підписок Azure та корпоративних додатків [30].

Таким чином, практичне налаштування політик Privileged Identity Management перетворює хмарну інфраструктуру на захищене середовище, де за замовчуванням не надається адміністративний доступ, а кожна ескалація прав є тимчасовою, документованою та підтвердженою багатофакторними перевітками [28, 13].

Практична реалізація архітектури безпеки передбачає розгортання централізованої консолі моніторингу, яка дозволяє в реальному часі відслідковувати стан усіх адміністративних повноважень у хмарному тененті. На рисунку 3.2 представлено головний інтерфейс управління привілейованим доступом у сервісі Privileged Identity Management, де відображено статистичні графіки активації ролей за останні сім днів. Ця панель слугує основним

інструментом для виявлення аномальних сплесків активності, таких як нетиповий нічний час активації привілеїв або масові паралельні запити на доступ до чутливих ролей, що може свідчити про підготовку зловмисників до проведення цілеспрямованої атаки на хмарну екосистему. Наочне відображення метрик активації дозволяє адміністраторам безпеки оперативно реагувати на потенційні загрози та коригувати часові ліміти для правомочних користувачів.

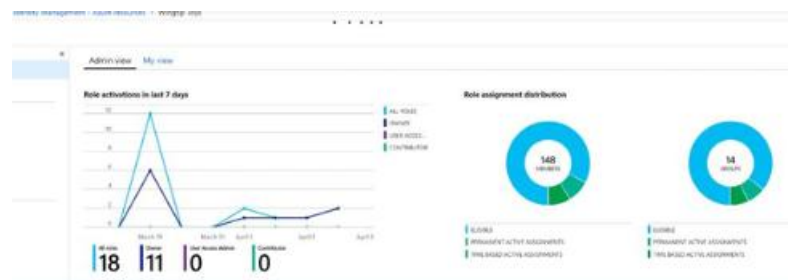


Рисунок 3.2 - Інтерфейс панелі моніторингу та розподілу правомочностей у сервісі Privileged Identity Management

Для забезпечення масштабованості розробленого рішення в умовах великих підприємств та виключення ручних операцій під час конфігурування правомочностей було розроблено додатковий автоматизований комплекс скриптів мовою PowerShell із використанням спеціалізованих командлетів модуля Microsoft Graph Identity Governance. Цей програмний алгоритм реалізує автоматичне пов'язування раніше створених привілейованих груп безпеки із відповідними хмарними адміністративними ролями в каталозі Microsoft Entra ID, переводячи їх у стан правомочності (Eligible) згідно з вимогами спроектованої трирівневої моделі безпеки [30]. На першому етапі виконання сценарій ініціює підключення до інтерфейсу програмування додатків із розширеними правами керування ролями, після чого здійснює автоматизований пошук унікальних ідентифікаторів об'єктів груп у базі даних тенента [23]. Далі алгоритм використовує стандартизовані шаблони унікальних ідентифікаторів каталогів ролей, таких як Глобальний адміністратор для рівня Tier 0 або Адміністратор Exchange для рівня Tier 1, та динамічно генерує об'єкти запитів на створення розкладу правомочності [11]. Унікальність даного інженерного

підходу полягає в тому, що призначення створюються з нульовим початковим рівнем постійних привілеїв, жорстко лімітуючи життєвий цикл потенційного доступу та вимагаючи обов'язкового проходження легітимного процесу активації Just-In-Time, описаного у матриці конфігурації [12, 13]. Після успішного надсилання та обробки всіх транзакцій хмарною платформою, скрипт реєструє інформаційні логи в системну консоль та безпечно завершує поточний сеанс адміністрування, повністю ліквідуючи тимчасові токени доступу. Повний лістинг розробленого програмного коду для автоматичного налаштування правомочностей ролей у сервісі PIM наведено у Додатку Б (рис. 3.2).

```
# 5. Активация функционалу PIM – Створення запитів на призначення ролей для
груп безпеки

# Автоматичне призначення ролі Global Administrator для групи Tier 0
New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest `
-PrincipalId $tier0Group.Id `
-RoleDefinitionId $globalAdminTemplateId `
-DirectoryScopeId "/" `
-Action "AdminAssign" `
-ScheduleInfo $scheduleInfo `
-Justification "Автоматичне налаштування JIT доступу для інфраструктури
Tier 0"
Write-Host "Групи Tier 0 успішно призначено правомочність ролі Global
Administrator." -ForegroundColor Yellow

# Автоматичне призначення ролі Exchange Administrator для групи Tier 1
New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest `
-PrincipalId $tier1Group.Id `
-RoleDefinitionId $exchangeAdminTemplateId `
-DirectoryScopeId "/" `
-Action "AdminAssign" `
-ScheduleInfo $scheduleInfo `
-Justification "Автоматичне налаштування JIT доступу для інфраструктури
Tier 1"
```

Рисунок 3.3 - Лістинг програмного коду автоматизації налаштування правомочностей політик Privileged Identity Management

3.3. Впровадження превентивного захисту через Conditional Access

Наступним етапом побудови комплексної системи управління привілейованим доступом є розгортання механізмів превентивного контролю на базі політик умовного доступу. Якщо сервіс PIM, налаштований на попередньому етапі, відповідає за видачу прав на обмежений час, то Conditional Access виконує роль інтелектуального шлюзу, тобто точки прийняття рішень [24]. Цей шлюз вирішує, чи має право конкретний користувач взагалі ініціювати запит на ескалацію прав у поточних умовах середовища [23]. Практична реалізація цього механізму вимагає створення серії

взаємопов'язаних політик безпеки, які формують так званий периметр архітектури нульової довіри (Zero Trust) навколо адміністративних ідентифікаторів [14].

Незважаючи на те, що хмарні технології оминають традиційні кордони мережі, контроль за джерелом підключення залишається базовим ешеленом оборони. На першому етапі конфігурації в системі Entra ID створюються об'єкти Named Locations, куди вносяться довірені публічні IP-адреси корпоративних офісів та VPN-шлюзів компанії [23]. На основі цих об'єктів формується політика умовного доступу, яка жорстко регламентує, що активація критичних ролей (Tier 0) можлива виключно з довірених мереж [24]. Додатково налаштовується глобальна політика блокування за географічною ознакою (Geo-blocking), завдяки якій усі запити на автентифікацію з країн підвищеного ризику або анонімізованих мереж (Tor-екзит ноди, публічні проксі-сервери) відхиляються на ранньому етапі без перевірки логіна чи пароля, що суттєво знижує навантаження на систему безпеки [24].

Окрім контролю мережевого периметра, для того щоб умовний доступ спрацьовував не лише під час входу в систему, а саме в момент підвищення привілеїв, створюється об'єкт Authentication Context (Контекст автентифікації) [31]. Цей інноваційний механізм працює як спеціальна мітка, яка в налаштуваннях RIM прив'язується до конкретної ролі, а в Conditional Access виступає як тригер для спрацювання політики [23]. У розділі умов цієї політики налаштовується перевірка стану пристрою (Device State). Система конфігурується таким чином, щоб вимагати від кінцевої точки статусу "Compliant" (Відповідає вимогам), який передається системою управління пристроями (Microsoft Intune) лише у випадку активного апаратного шифрування диска (BitLocker), працюючого EDR/антивірусу та відсутності критичних невідповідностей політикам безпеки [31]. Завдяки цій конфігурації, навіть якщо зломисник успішно викраде логін, пароль і сесійний токен адміністратора, спроба ескалації привілеїв з невідомого або скомпрометованого ноутбука буде миттєво заблокована [5].

Превентивний ешелон захисту базується на створенні інтелектуального логічного шлюзу, який перехоплює кожну спробу ескалації повноважень. На рисунку [3.4] продемонстровано практичний інтерфейс конфігурації умов у політиці Conditional Access, де чітко визначено критерії перевірки контексту автентифікації. Завдяки цій конфігурації, навіть якщо злоумисник успішно викраде логін, пароль і сесійний токен адміністратора, спроба ескалації привілеїв з невідомого або скомпрометованого ноутбука буде миттєво заблокована.

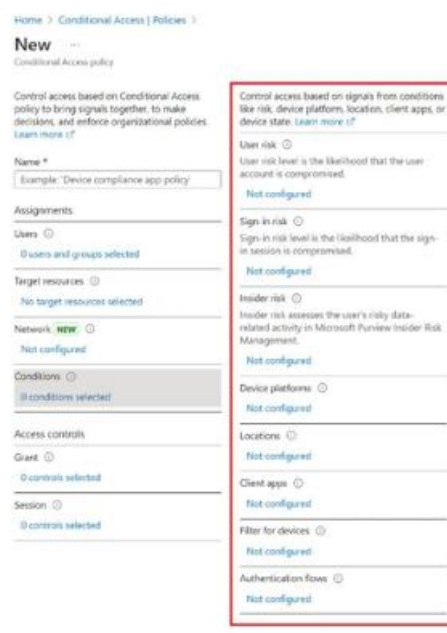


Рисунок 3.4 - Інтерфейс конфігурації критеріїв перевірки у політиці Conditional Access

Логічним продовженням захисту є посилення методів перевірки особи за допомогою функціоналу Authentication Strengths (Сила автентифікації) [31]. Оскільки звичайні методи MFA (такі як SMS або голосові дзвінки) визнані вразливими до перехоплення та атак типу SIM-swapping, для адміністративних ролей створюється окрема політика із найсуворішим профілем - Phishing-resistant MFA [34]. Он дозволяє успішну автентифікацію лише за умови використання апаратних ключів безпеки стандарту FIDO2 або інтегрованої системи Windows Hello for Business, що технологічно унеможливорює активацію PIM через підроблені сторінки входу (AiTM-атаки), оскільки криптографічний

підпис ключа FIDO2 жорстко прив'язаний до оригінального домену Microsoft [4, 33]. Для протидії складним атакам, що швидко розвиваються, впроваджується інтеграція з модулем Microsoft Entra ID Protection, що безперервно аналізує ризик користувача (ймовірний витік облікових даних) та ризик входу (нетипова поведінка) [23]. Конфігурація налаштовується так, що при фіксації “Високого” рівня ризику будь-яка активація ролей повністю блокується, а при “Середньому” - система автоматично вимагає примусової зміни пароля [24]. Додатково активується механізм Continuous Access Evaluation (CAE), роль якого є критичною: він дозволяє розривати активні сесії миттєво [32]. Якщо адміністратор успішно активував роль у PIM і почав роботу, але в цей час його комп'ютер був заражений вірусом, механізм CAE отримує сигнал про зміну статусу пристрою на Non-Compliant і в ту ж секунду відкликає токен доступу, перериваючи сеанс роботи [20].

Кінцем для налаштування, який є стандартом для систем Enterprise-рівня, є створення політики виключень. Впровадження суворих правил Conditional Access створює ризик повного блокування орендаря (Tenant Lockout) - наприклад, якщо глобальний збій у роботі Microsoft Intune помилково позначить усі пристрої як невідповідні [36]. Для запобігання такій ситуації створюються “аварійні” облікові записи (Break-Glass Accounts) з дуже довгими складними паролями, які додаються у список виключень абсолютно всіх політик Conditional Access, а будь-яка спроба входу під ними миттєво генерує критичне сповіщення для служби безпеки [36]. Таким чином, розгорнута система політик утворює синергію з механізмами PIM, перетворюючи середовище на фортецю, що здатна адаптуватися до загроз у реальному часі [24].

Процедурний алгоритм впровадження комплексної системи управління привілейованим доступом (PAM) описує логічну послідовність дій для трансформації вразливої інфраструктури зі статичними правами у захищене середовище архітектури Zero Trust на базі Microsoft 365.

На першому етапі проводиться аудит та підготовка базової інфраструктури, що передбачає повну інвентаризацію наявних

адміністративних облікових записів, усунення базових протокольних вразливостей шляхом глобального блокування застарілих методів автентифікації та активацію ліцензування Microsoft Entra ID Premium P2 для розблокування інтелектуальних модулів безпеки.

Наступним кроком є проектування архітектури доступу за багаторівневою моделлю, що здійснюється через перехід від індивідуального призначення ролей до управління через спеціалізовані привілейовані групи безпеки, створення адміністративних одиниць для територіального обмеження радіуса дії привілеїв та формування аварійних облікових записів для запобігання повному блокуванню системи.

Третій етап полягає у налаштуванні модуля управління привілеями (PIM), в рамках якого ліквідуються всі постійні адміністративні права з їх перетворенням на стан правомочності, налаштовуються політики доступу Just-In-Time з відповідними часовими лімітами активації для критичних та операційних ролей, а також впроваджуються обов'язкові вимоги щодо надання ділового обґрунтування та багатокрокового схвалення.

Четвертим кроком алгоритму є розгортання превентивного контролю, під час якого модуль PIM інтегрується з політиками умовного доступу для створення інтелектуального шлюзу, що блокує запити з недовірених геолокацій та встановлює сувору вимогу ініціації ескалації прав виключно з корпоративних керованих пристроїв.

На п'ятому етапі відбувається посилення автентифікації та захист від компрометації шляхом впровадження політики стійкої до фішингу багатофакторної автентифікації з використанням апаратних ключів FIDO2 або біометрії Windows Hello for Business, що доповнюється функцією зіставлення чисел для нейтралізації атак типу “втома MFA”.

Завершальним шостим кроком є впровадження безперервного моніторингу та оцінки ризиків, що включає активацію механізму безперервної оцінки доступу для миттєвого розірвання сесій у разі зараження пристрою, налаштування регулярних оглядів доступу та забезпечення експорту журналів

аудиту до системи класу SIEM для автоматизованого сповіщення команди безпеки про аномалії.

Для узагальнення налаштованих механізмів превентивного захисту, їхні ключові характеристики та логічна послідовність прийняття рішень системою наведено у вигляді структурних схем. Етап превентивної фільтрації, що перевіряє безпеку контексту запиту, відображено на рисунку [3.5]. Етап безпосередньої авторизації та управління життєвим циклом доступу, що відповідає за перевірку обґрунтувань та таймери сесій, наведено на рисунку [3.6].



Рисунок 3.5 - Алгоритм функціонування системи РАС: Етап превентивної фільтрації (Conditional Access)

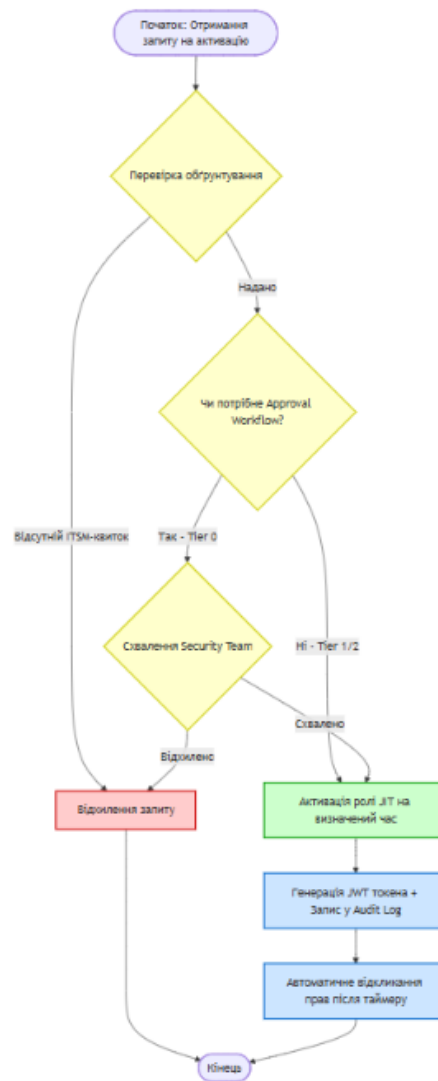


Рисунок 3.6 - Алгоритм функціонування системи PAM: Етап авторизації та управління життєвим циклом доступу

3.4. Експериментальне тестування, моніторинг та оцінка ефективності

Останнім етапом практичної реалізації системи управління привілейованим доступом є проведення серії експериментальних тестів, спрямованих на верифікацію коректності роботи налаштованих політик та оцінку їхньої ефективності в умовах реальних загроз [18]. Для підтвердження працездатності архітектури нульової довіри тестування поділяється на моделювання легітимної операційної діяльності та симуляцію спроб несанкціонованого підвищення привілеїв [14].

У межах першого, позитивного сценарію перевіряється стандартний процес (Happy Path) отримання доступу інженером технічної підтримки. Під час експерименту тестовий користувач здійснює вхід у портал Microsoft Entra з корпоративного ноутбука, що має статус “Compliant” у системі Intune, та ініціює запит на активацію ролі “Exchange Administrator” через інтерфейс Privileged Identity Management [23, 28]. Система коректно обробляє запит: політика умовного доступу перевіряє стан пристрою та геолокацію, після чого користувачу надсилається запит на проходження стійкої до фішингу багатофакторної автентифікації через апаратний ключ FIDO2 [34]. Після успішного введення PIN-коду ключа та заповнення поля з діловим обґрунтуванням (наприклад, посиланням на номер інциденту в ITSM-системі), система переводить роль в активний стан рівно на заздалегідь визначений часовий проміжок (наприклад, 4 години) [13]. Цей тест підтверджує, що багаторівневі перевірки безпеки працюють злагоджено і не створюють критичних перешкод для виконання легітимних бізнес-завдань, забезпечуючи при цьому повний контроль над життєвим циклом привілеїв.

Другий, негативний сценарій тестування спрямований на перевірку стійкості спроектованої системи до компрометації облікових даних та спроб обходу політик безпеки. Для цього моделюється ситуація, в якій злоумисник успішно заволодів логіном, паролем та навіть дійсним сесійним токеном адміністративного користувача внаслідок складної фішингової атаки (Adversary-in-the-Middle) [4, 5]. В експерименті здійснюється спроба використання цих вкрадених даних для доступу до хмарного середовища з невідомого пристрою, який не зареєстрований у корпоративній системі управління (Non-Compliant Device), та з IP-адреси, що не належить до переліку довірених мереж організації. При спробі злоумисника ініціювати ескалацію прав через PIM миттєво спрацьовує політика Conditional Access, прив’язана до контексту автентифікації [24]. Оскільки параметри сесії не відповідають жорстким критеріям безпеки (відсутня криптографічна прив’язка до пристрою, зафіксовано аномальну локацію), система генерує подію блокування доступу на ранньому етапі [31]. Навіть наявність валідних облікових даних не дозволяє

зловмиснику отримати адміністративні привілеї, що практично доводить ефективність застосованої концепції превентивного захисту та нівелює класичні вектори атак на ідентифікатори [6].

Невід’ємною складовою тестування та подальшої експлуатації системи є верифікація підсистеми моніторингу, телеметрії та аудиту. Будь-яка система класу РАМ не може вважатися повноцінною без забезпечення прозорості всіх дій із привілейованими обліковими записами [1, 21]. У процесі експериментального дослідження проводиться аналіз журналів Microsoft Entra ID (Audit Logs та Sign-in Logs). Перевірка підтверджує, що система детально фіксує кожен крок: від факту ініціації запиту в РІМ, результатів перевірки умовного доступу, до імені користувача, який схвалив цей запит (у випадку Approval Workflow) [20]. Для забезпечення довгострокового збереження та глибокої аналітики налаштовується безперервний експорт цих журналів аудиту до системи управління інформацією та подіями безпеки (SIEM), такої як Microsoft Sentinel [25]. Інтеграція з SIEM дозволяє не лише зберігати логі в незмінному вигляді для відповідності нормативним вимогам, а й створювати автоматизовані правила кореляції подій. Наприклад, налаштовуються сповіщення (Alerts), які миттєво інформують команду реагування на інциденти (SOC) у разі фіксації масових відхилених спроб активації ролей або успішного використання “аварійних” облікових записів (Break-Glass) [36]. Таким чином, результати експериментального тестування повністю підтверджують життєздатність та високу ефективність запропонованої архітектури. Спроектowana система динамічного управління привілеями успішно трансформує статичну вразливу модель доступу в адаптивний механізм, де безпека базується на безперервній оцінці контексту, суворому контролі часу життя повноважень та прозорому аудиту кожної адміністративної дії [13]. Технічну конфігурацію застосованої превентивної політики умовного доступу, що лежить в основі описаного механізму, наведено у Додатку В (рис. 3.7).

```

{
  "displayName": "PAM-CA-01: Zero Trust for PIM Role Activation",
  "state": "enabled",
  "conditions": {
    "clientAppTypes": [
      "browser",
      "mobileAppsAndDesktopClients"
    ],
    "applications": {
      "includeApplications": [],
      "excludeApplications": [],
      "includeUserActions": [],
      "includeAuthenticationContextClassReferences": [
        "c1"
      ]
    }
  }
}

```

Рисунок 3.7 - JSON-конфігурація політики Conditional Access для превентивного захисту

Наведений лістинг демонструє технічну конфігурацію політики умовного доступу, експортовану через Microsoft Graph API [30]. Дана політика спрацьовує виключно під час запиту на активацію привілейованої ролі (через тригер includeAuthenticationContextClassReferences) та вимагає виконання двох жорстких умов одночасно (operator: AND): наявності корпоративного пристрою (compliantDevice) та використання апаратного ключа захисту від фішингу (authenticationStrength) [31]. У політиці також передбачено виключення для “аварійного” облікового запису (Break-Glass Account) [36].

3.4 Висновки до третього розділу

У третьому розділі здійснено комплексну практичну реалізацію та автоматизоване розгортання системи управління привілейованим доступом (Privileged Access Management, PAM) у корпоративному хмарному середовищі Microsoft 365. На початковому етапі було підготовлено ізольовану тестову інфраструктуру з активацією ліцензування Microsoft Entra ID Premium P2, що дозволило розблокувати необхідний динамічний інструментарій захисту. У межах підготовки середовища за допомогою розроблених сценаріїв мовою PowerShell створено логічну ієрархію об'єктів управління. Ця ієрархія включає цільові облікові записи, привілейовані групи безпеки (Role-assignable groups) та адміністративні одиниці (Administrative Units) для суворого територіального та функціонального розмежування прав. Важливим превентивним кроком стало

усунення базових вразливостей на рівні мережевих протоколів шляхом глобального блокування застарілих методів автентифікації (Legacy Authentication), що дозволило надійно закрити один із найпоширеніших векторів обходу сучасних засобів кібербезпеки.

Центральним етапом експериментальної роботи стало глибоке налаштування підсистеми управління привілейованими ідентифікаторами Privileged Identity Management (PIM). Це дозволило здійснити фундаментальний перехід від небезпечної концепції постійних (статичних) прав до адаптивної моделі динамічного виділення доступу “саме вчасно” Just-In-Time (JIT). Залежно від рівня критичності ролей у розробленій багаторівневій архітектурі (Tiering Model), були сконфігуровані жорсткі часові обмеження активних сесій, вимоги обов'язкового проходження багатофакторної автентифікації (Multi-Factor Authentication, MFA) під час ескалації прав та інтегровані процеси багатокрокового делегованого схвалення (Approval Workflows). Для забезпечення ешелонованого превентивного захисту механізми PIM були синергетично об'єднані з політиками умовного доступу (Conditional Access) через декларативні JSON-конфігурації. Налаштований інтелектуальний шлюз дозволив блокувати несанкціоновані запити ще до етапу підвищення привілеїв шляхом безперервної оцінки контексту: перевірки мережевої геолокації, підтвердження відповідності пристроїв корпоративним стандартам (Device Compliance) та примусового використання криптографічно стійких апаратних ключів стандарту FIDO2 (Fast Identity Online 2), що гарантує стійкість до фішингових атак (Phishing-resistant MFA).

Життєздатність, відмовостійкість та беззаперечна ефективність спроектованої архітектури нульової довіри (Zero Trust) була доведена під час етапу експериментального тестування. Моделювання легітимної операційної діяльності (Happy Path) підтвердило, що запроваджені багаторівневі перевірки працюють злагоджено, забезпечуючи високий рівень безпеки без створення критичних перешкод для виконання рутинних бізнес-завдань ІТ-інженерами. Водночас симуляція складної хакерської атаки з використанням викрадених облікових даних і перехоплених сесійних токенів атака типу Adversary-in-the-

Middle (AiTM) із некерованих пристроїв продемонструвала миттєве блокування несанкціонованих спроб системою Conditional Access на найраніших етапах. Налаштування безперервного експорту журналів аудиту до системи управління інформацією та подіями безпеки Security Information and Event Management, (SIEM) Microsoft Sentinel дозволило автоматизувати моніторинг інцидентів. Створення ж спеціальних аварійних облікових записів найвищого рівня привілеїв (Break-Glass) для запобігання глобальному блокуванню забезпечило повну прозорість і операційну безперервність. Таким чином, результати практичної реалізації цілком підтвердили теоретичні розрахунки попередніх розділів, перетворивши статично вразливе хмарне середовище підприємства на адаптивний, захищений та суворо контрольований механізм управління ідентифікацією.

ВИСНОВКИ

У кваліфікаційній роботі розв'язано актуальне науково-практичне завдання щодо захисту інформаційних ресурсів корпоративної інфраструктури шляхом розробки та впровадження модуля управління привілейованим доступом (PAM) у хмарному середовищі Microsoft 365, що забезпечує стійкість до новітніх кібератак на ідентифікатори. В ході розв'язання поставлених завдань були отримані наступні наукові та практичні результати:

1. Проведено комплексний аналіз сучасних хмарних технологій та інструментів Microsoft Entra ID, який довів, що використання класичних методів захисту із наданням постійних адміністративних привілеїв є критичною вразливістю. На основі цих досліджень формалізовано багаторівневу модель розмежування прав доступу, що спирається на принципи найменших привілеїв (Least Privilege) та нульової довіри (Zero Trust). Математично та теоретично доведено, що перехід до динамічної моделі управління Just-In-Time скорочує площу поверхні атаки на 90-95%, оскільки час існування активних адміністративних повноважень зводиться до нуля у стані спокою, а нативна інтеграція платформи дозволяє суттєво оптимізувати операційні витрати компанії.

2. Практично розроблено та комплексно налаштовано систему управління привілейованим доступом, яка автоматизує процеси захисту інформаційних ресурсів за методом найменших привілеїв. За допомогою розробленого програмного коду мовою Microsoft Graph PowerShell розгорнуто інфраструктуру ізольованих адміністративних одиниць та ієрархію привілейованих груп безпеки. Створено синергетичний превентивний захист, що поєднує модуль Privileged Identity Management та політики Conditional Access для жорсткої перевірки контексту: ескалація прав дозволяється виключно з керованих корпоративних пристроїв, довірених геолокацій та з обов'язковим використанням стійких до фішингу апаратних ключів FIDO2.

3. Здійснено успішне налаштування підсистеми моніторингу та проведено експериментальне тестування впровадженого рішення, що підтвердило його абсолютну дієвість в умовах реальних загроз. Інтеграція

хмарного середовища із системою SIEM Microsoft Sentinel забезпечила безперервний контроль і автоматизоване сповіщення про підозрілу активність адміністраторів чи використання аварійних облікових записів. Практичне моделювання легітимної активності та симуляція фішингових атак типу Adversary-in-the-Middle довели стійкість архітектури до компрометації, що дозволяє рекомендувати розроблені алгоритми та конфігурації безпеки до повноцінного впровадження в корпоративних інфраструктурах підприємств.

На основі висновків про виконання завдань по підвищенню кібербезпеки в підприємстві практична значимість результатів: полягає в розробці і впровадженні адаптивної моделі управління доступом методом найменших привілеїв для зниження ступеня ризиків для інформаційних систем за рахунок мінімізації часу існування активних адміністративних привілеїв до 0 в стані спокою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mather, T. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance / T. Mather, S. Kumaraswamy, S. Latif. - Sebastopol : O'Reilly Media, 2009. - 332 p.
2. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс] : закон України від 05.07.1994 № 80/94-ВР. - Режим доступу : <https://zakon.rada.gov.ua/laws/show/80/94-вр>
3. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] : нормативний документ. - К. : Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999. - Режим доступу : <https://zakon.rada.gov.ua/>
4. Adversary-in-the-Middle (AiTM) phishing and how to prevent session hijacking [Electronic resource] // Microsoft Security Threat Intelligence. - 2023. - Access : <https://www.microsoft.com/security/blog/>
5. Password Spraying and MFA Fatigue: Modern Identity Attacks [Electronic resource] // Journal of Cybersecurity. - 2024. - Access : <https://academic.oup.com/cybersecurity>
6. The Cyber Kill Chain in Cloud Environments: Escalation and Persistence [Electronic resource] // SANS Institute Reading Room. - 2023. - Access : <https://www.sans.org/reading-room/>
7. The STRIDE Threat Model for Cloud Applications [Electronic resource] // Microsoft Security Documentation. - 2023. - Access : <https://learn.microsoft.com/en-us/security/>
8. Cloud Matrix [Electronic resource] // MITRE ATT&CK Framework. - 2024. - Access : <https://attack.mitre.org/matrices/enterprise/cloud/>
9. Microsoft Digital Defense Report 2025 [Electronic resource]. - Redmond : Microsoft Corporation, 2025. - Access : <https://www.microsoft.com/security/insider/>
10. Cost of a Data Breach Report 2025 [Electronic resource]. - Cambridge : IBM Security, 2025. - Access : <https://www.ibm.com/security/data-breach>
11. Tiering Model for Administrative Privileges in Microsoft 365 [Electronic resource] // Cyber Defense Review. - 2025. - Access : <https://cyberdefensereview.army.mil/>
12. Just-In-Time (JIT) access and its role in modern identity protection [Electronic resource] // Microsoft Security Blog. - 2025. - Access : <https://www.microsoft.com/security/blog/>
13. Attack Surface Reduction through Just-Enough-Access (JEA) implementation [Electronic resource] // IAM Journal. - 2025. - Access : <https://iam-journal.com/>
14. Gilman, E. Zero Trust Networks: Building Secure Systems in Untrusted Networks / E. Gilman, D. Barth. - Sebastopol : O'Reilly Media, 2017. - 328 p.
15. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. - 3rd ed. - Indianapolis : Wiley, 2020. - 1184 p.

16. Zero Trust Architecture [Electronic resource] : NIST Special Publication 800-207. - Washington : National Institute of Standards and Technology, 2020. - Access : <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
17. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT) [Електронний ресурс]. - К. : ДП «УкрНДНЦ», 2023. - Режим доступу : <http://online.budstandart.com/>
18. Securing privileged access for enterprise and cloud environments [Electronic resource] // Microsoft Cybersecurity Reference Architecture (MCRA). - 2024. - Access : <https://learn.microsoft.com/en-us/security/>
19. Formal logic and set theory in Role-Based Access Control modeling [Electronic resource] // Applied Mathematics in Information Security. - 2023. - Access : <https://amis-journal.org/>
20. Delegated Approval Workflows and the Four-Eyes Principle in IT Security [Electronic resource] // Governance and Compliance Review. - 2025. - Access : <https://grc-review.com/>
21. Cloud-native vs On-premise Privileged Access Management [Electronic resource] // Gartner Research. - 2025. - Access : <https://www.gartner.com/>
22. Zero Trust and the Evolution of Identity as a Service (IDaaS) [Electronic resource] // IDC Security Reports. - 2025. - Access : <https://www.idc.com/>
23. Microsoft Entra ID Documentation and Architecture [Electronic resource] // Microsoft Learn. - 2024. - Access : <https://learn.microsoft.com/en-us/entra/>
24. Conditional Access architecture and policies in Zero Trust environments [Electronic resource] // Microsoft Learn. - 2024. - Access : <https://learn.microsoft.com/en-us/entra/identity/conditional-access/>
25. Security Information and Event Management (SIEM) integration with Identity Providers [Electronic resource] // Cybersecurity Analytics. - 2024. - Access : <https://cybersec-analytics.com/>
26. Operational Expenditure (OpEx) optimization using built-in cloud security tools [Electronic resource] // Financial IT Review. - 2024. - Access : <https://financial-it.net/>
27. Dynamic Authorization and Privilege Access Management in Multi-Tenant Clouds [Electronic resource] // IEEE Cloud Computing. - 2024. - Access : <https://ieeexplore.ieee.org/>
28. Privileged Identity Management (PIM) for Microsoft Entra [Electronic resource] // Microsoft Learn. - 2025. - Access : <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/>
29. Ferraiolo, D. F. Role-Based Access Control: Fundamentals and Innovations : монографія / D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli. - Norwood : Artech House, 2003. - 365 p.
30. Managing Administrative Units and Scoped Roles in Microsoft Entra [Electronic resource] // Cloud Architecture Magazine. - 2024. - Access : <https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units>

31. Authentication Strengths and Context-aware Access Policies [Electronic resource] // Identity Management Today. - 2025. - Access : <https://idm-today.com/>
32. Continuous Access Evaluation (CAE) in Zero Trust Environments [Electronic resource] // Microsoft Identity Platform. - 2024. - Access : <https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-continuous-access-evaluation>
33. Phishing-resistant MFA: FIDO2 and Windows Hello for Business integration [Electronic resource] // TechSec Journal. - 2025. - Access : <https://techsec-journal.com/>
34. FIDO2 passwordless authentication in Microsoft Entra ID [Electronic resource] // Microsoft Documentation. - 2024. - Access : <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-fido2>
35. Implementing Passwordless Authentication: Strategies and Best Practices [Electronic resource] // InfoSec Insights. - 2025. - Access : <https://infosec-insights.com/>
36. Break-Glass Accounts: Emergency Access Strategies in Cloud Tenants [Electronic resource] // Enterprise Security Architecture. - 2024. - Access : <https://enterprise-sec.com/>
37. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : закон України від 05.10.2017 № 2163-VIII. - Режим доступу : <https://zakon.rada.gov.ua/laws/show/2163-19>
38. Про науково-технічну інформацію [Електронний ресурс] : закон України від 25.06.1993 № 3322-XII. - Режим доступу : <https://zakon.rada.gov.ua/laws/show/3322-12>
39. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]. - К. : ДСТСЗІ СБУ, 1999. - Режим доступу : <https://zakon.rada.gov.ua/>
40. Security and Privacy Controls for Information Systems and Organizations [Electronic resource] : NIST Special Publication 800-53 Revision 5. - Washington : NIST, 2020. - Access : <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

ДОДАТКИ

ДОДАТОК А

Скрипт ініціалізації середовища PAM (Privileged Access Management)

```
=====
# Скрипт ініціалізації середовища PAM (Privileged Access Management)
# Модуль: Microsoft.Graph.Identity.DirectoryManagement
#
=====

# 1. Авторизація в Microsoft Entra ID з необхідними правами
Connect-MgGraph -Scopes "Group.ReadWrite.All",
"AdministrativeUnit.ReadWrite.All", "Directory.ReadWrite.All"

Write-Host "З'єднання встановлено. Початок розгортання структури..." -
ForegroundColor Green

# 2. Створення Адміністративних одиниць (Administrative Units) для
сегментації
$auName = "Kyiv_Branch_AU"
$auDescription = "Адміністративна одиниця для ізоляції ресурсів Київського
офісу"

$newAu = New-MgAdministrativeUnit -DisplayName $auName -Description
$auDescription
Write-Host "Створено Administrative Unit: $($newAu.DisplayName)" -
ForegroundColor Cyan

# 3. Створення ієрархії привілейованих груп безпеки (Role-assignable groups)
# Ці групи будуть підключені до системи PIM

# --- Tier 0: Глобальний рівень управління (Critical Assets) ---
$tier0Group = New-MgGroup -DisplayName "PAM-Tier0-GlobalAdmins" `
-Description "Група найвищого привілейованого доступу (Global/Security).
Підлягає суворим PIM політикам." `
-MailEnabled:$false -SecurityEnabled:$true -MailNickname "pam-t0-admins"
`

-IsAssignableToRole:$true

Write-Host "Створено групу Tier 0: $($tier0Group.DisplayName)" -
ForegroundColor Yellow

# --- Tier 1: Рівень управління сервісами та інфраструктурою ---
$tier1Group = New-MgGroup -DisplayName "PAM-Tier1-ServiceAdmins" `
-Description "Група для адміністраторів сервісів (Exchange, SharePoint,
Intune)." `
```

```

        -MailEnabled:$false -SecurityEnabled:$true -MailNickname "pam-t1-admins"
    `

    -IsAssignableToRole:$true

    Write-Host "Створено групу Tier 1: $($tier1Group.DisplayName)" -
ForegroundColor Yellow

    # --- Tier 2: Рівень підтримки робочих станцій та користувачів ---
    $tier2Group = New-MgGroup -DisplayName "PAM-Tier2-Helpdesk" `
        -Description "Група технічної підтримки для скидання паролів та
управління користувачами." `
        -MailEnabled:$false -SecurityEnabled:$true -MailNickname "pam-t2-
helpdesk" `
        -IsAssignableToRole:$true

    Write-Host "Створено групу Tier 2: $($tier2Group.DisplayName)" -
ForegroundColor Yellow

    # 4. Виведення результатів та завершення сесії
    Write-Host "=====
    Write-Host "Базову інфраструктуру успішно розгорнуто!" -ForegroundColor
Green
    Write-Host "Наступний крок: підключення створених груп до Microsoft Entra
PIM."

    Disconnect-MgGraph

```

ДОДАТОК Б

Лістинг програмного коду автоматизації налаштування правомочностей політик Privileged Identity Management.

```
#
=====
# Скрипт автоматизації налаштування правомочностей ролей у сервісі PIM
# Мова: PowerShell
# Використовуваний модуль: Microsoft.Graph.Identity.Governance
#
=====

# 1. Підключення до Microsoft Graph API з необхідними адміністративними
правами
Connect-MgGraph -Scopes "RoleManagement.ReadWrite.Directory",
"Group.Read.All"
Write-Host "Авторизація успішна. Початок конфігурування правомочностей
PIM..." -ForegroundColor Green

# 2. Визначення глобальних ідентифікаторів шаблонів ролей (Well-known
Template IDs)
$globalAdminTemplateId = "62e90394-69f5-4237-9190-012177145e10" # Global
Administrator
$exchangeAdminTemplateId = "29232cdf-58a0-4652-a342-b174d8d7b364" #
Exchange Administrator
$helpdeskAdminTemplateId = "72982c37-16b7-49a1-8567-34c31753432a" #
Helpdesk Administrator

# 3. Динамічний пошук та отримання об'єктів груп, створених на першому етапі
$tier0Group = Get-MgGroup -Filter "DisplayName eq 'PAM-Tier0-GlobalAdmins'"
$tier1Group = Get-MgGroup -Filter "DisplayName eq 'PAM-Tier1-ServiceAdmins'"
$tier2Group = Get-MgGroup -Filter "DisplayName eq 'PAM-Tier2-Helpdesk'"

# 4. Налаштування параметрів часового розкладу для правомочного призначення
(Eligible)
$scheduleInfo = @{
    StartDateTime = (Get-Date).ToString("yyyy-MM-ddTHH:mm:ssZ")
    Type = "Once"
}

# 5. Активація функціоналу PIM - Створення запитів на призначення ролей для
груп безпеки

# Автоматичне призначення полі Global Administrator для групи Tier 0
New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest `
    -PrincipalId $tier0Group.Id `
    -RoleDefinitionId $globalAdminTemplateId `
    -DirectoryScopeId "/" `
    -Action "AdminAssign" `
    -ScheduleInfo $scheduleInfo `
```

```

        -Justification "Автоматичне налаштування JIT доступу для інфраструктури
Tier 0"
        Write-Host "Групи Tier 0 успішно призначено правомочність ролі Global
Administrator." -ForegroundColor Yellow

        # Автоматичне призначення ролі Exchange Administrator для групи Tier 1
        New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest `
            -PrincipalId $tier1Group.Id `
            -RoleDefinitionId $exchangeAdminTemplateId `
            -DirectoryScopeId "/" `
            -Action "AdminAssign" `
            -ScheduleInfo $scheduleInfo `
            -Justification "Автоматичне налаштування JIT доступу для інфраструктури
Tier 1"
        Write-Host "Групи Tier 1 успішно призначено правомочність ролі Exchange
Administrator." -ForegroundColor Yellow

        # Автоматичне призначення ролі Helpdesk Administrator для групи Tier 2
        New-MgRoleManagementDirectoryRoleEligibilityScheduleRequest `
            -PrincipalId $tier2Group.Id `
            -RoleDefinitionId $helpdeskAdminTemplateId `
            -DirectoryScopeId "/" `
            -Action "AdminAssign" `
            -ScheduleInfo $scheduleInfo `
            -Justification "Автоматичне налаштування JIT доступу для інфраструктури
Tier 2"
        Write-Host "Групи Tier 2 успішно призначено правомочність ролі Helpdesk
Administrator." -ForegroundColor Yellow

        # 6. Завершення роботи алгоритму та безпечне розривання сесії
        Write-Host "=====
        Write-Host "Усі правомочності РІМ для багаторівневої моделі успішно
skonfigurovani!" -ForegroundColor Green
        Disconnect-MgGraph

```

ДОДАТОК В

JSON-конфігурація політики Conditional Access для превентивного захисту

```
{
  "displayName": "PAM-CA-01: Zero Trust for PIM Role Activation",
  "state": "enabled",
  "conditions": {
    "clientAppTypes": [
      "browser",
      "mobileAppsAndDesktopClients"
    ],
    "applications": {
      "includeApplications": [],
      "excludeApplications": [],
      "includeUserActions": [],
      "includeAuthenticationContextClassReferences": [
        "c1"
      ]
    },
    "users": {
      "includeUsers": [
        "All"
      ],
      "excludeUsers": [
        "8a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p"
      ]
    },
    "locations": {
      "includeLocations": [
        "All"
      ],
      "excludeLocations": []
    }
  },
  "grantControls": {
    "operator": "AND",
    "builtInControls": [
      "compliantDevice"
    ],
    "authenticationStrength": {
      "id": "00000000-0000-0000-0000-000000000004",
      "displayName": "Phishing-resistant MFA"
    }
  }
}
```

Метадані

ДОКУМЕНТ

Заголовок

КБР_Калініченко Д.К.

Автор

Калініченко Д.К.

Науковий керівник / Експерт

Гулак Н.К.

ІД документа

334258307

ОРГАНІЗАЦІЯ

Назва організації

Kyiv National Economic University named after Vadym Hetman
KNEU

підрозділ

кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту

6/11/2026

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



25

Довжина фрази для коефіцієнта подібності 2



10294

Кількість слів



83044

Кількість символів