**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ**

**Автоматизації і інформаційних технологій**
(факультет)

**Кафедра кібербезпеки та комп'ютерної інженерії**
(назва кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

на тему:

Технологія розмежування доступу з використанням сервісу централізованого зберігання паролей

Малінський Микита Сергійович
(прізвище, ім'я та по батькові здобувача повністю)

Київ 2025 р.

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ**

**Автоматизації і інформаційних технологій**

(факультет)

**Кафедра кібербезпеки та комп'ютерної інженерії**

(назва кафедри)

**ЗАТВЕРДЖУЮ**
Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ

_____
„___" _____20___ року

# КВАЛІФІКАЦІЙНА РОБОТА ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР

Технологія розмежування доступу з використанням сервісу централізованого зберігання паролей

(назва)

*Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.*

Здобувач Малінський Микита Сергійович
(прізвище, ім'я та по батькові повністю)
125 "Кібербезпека та захист інформації"
(спеціальність)
Безпека інформаційних і комунікаційних систем
(освітня програма)
Група БІКСм-24
Керівник Шабала Є.Є.
(прізвище та ініціали)
кандитат технічних наук, доцент
(вчене звання, науковий ступінь)
Рецензент к.т.н, професор Терентьєв О.О.
(прізвище та ініціали)

*Ідентичність підтверджую*

Київ 2025 р.

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ**

Факультет: автоматизації і інформаційних технологій
Кафедра: кібербезпеки та комп'ютерна інженерія
Освітній рівень: магістр
Спеціальність: кібербезпека та захист інформації
ОПП: безпека інформаційних систем і комунікаційних систем

**ЗАТВЕРДЖУЮ**

Завідувач кафедри
к.т.н., доцент Максим ДЕЛЕМБОВСЬКИЙ

_____
„___"_____20___ року

**З А В Д А Н Н Я**
**ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ МАГІСТР**

Малінський Микита Сергійович
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи Технологія розмежування доступу з використанням сервісу централізованого зберігання паролей
затверджена наказом ректора КНУБА № 165/23.2/25 від « 30 » 09 2025року
2. Керівник роботи
Шабала Євгенія Євгенівна, к.т.н., доцент
( прізвище, ім'я та по батькові, науковий ступінь, вчене звання)
3. Термін подання здобувачем роботи до захисту_____
4. Зміст пояснювальної записки за розділами:
Р. 1. АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ
Р. 2. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ
Р. 3. ПРОЕКТНА ТА ПРАКТИЧНА ЧАСТИНА
5. Графічний матеріал за розділами:
Р. 1. 4 рисунки, 4 таблиці
Р. 2. 1 рисунок, 6 таблиць
Р. 3. 9 рисунків, 1 таблиця
6. Консультанти розділів кваліфікаційної випускної роботи

| Розділи | Прізвища, ініціали та посади консультанта | Перевірив | |
|---|---|---|---|
| | | дата | підпис |
| Розділ 1. | | | |
| Розділ 2. | | | |
| Розділ 3. | | | |

7. Календарний план виконання роботи:

| Види робіт та їх зміст | Дата виконання |
|---|---|
| Розділ 1. | Вересень 2025 р. |
| Розділ 2. | Жовтень 2025 р. |
| Розділ 3. | Жовтень 2025 р. |
| Остаточне оформлення роботи | Листопад 2025 р. |
| Направлення роботи на рецензування, перевірку на плагіат | Грудень 2025 р. |
| Попередній захист роботи на кафедрі | Грудень 2025 р. |

8. Дата видачі завдання 30 вересня 2025 року

Керівник _____ Шабала Є.Є.
(підпис) (прізвище та ініціали)

Здобувач _____ Малінський М.С.
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Малінський М.С. «Технологія розмежування доступу з використанням сервісу централізованого зберігання паролів».

Тема дипломного проєкту присвячена дослідженню та розробці технології розмежування доступу до інформаційних ресурсів із використанням сервісу централізованого зберігання паролів. У роботі розглянуто актуальні проблеми захисту облікових даних в корпоративних інформаційних системах та проаналізовано сучасні загрози, пов’язані з несанкціонованим доступом і компрометацією паролів.

Проведено аналіз сучасних моделей контролю доступу, зокрема RBAC та ABAC, а також вивчено підходи до централізованого управління обліковими даними. Описано архітектуру системи на основі сервісу Passbolt, принципи його інтеграції з існуючими інформаційними системами та методи криптографічного захисту даних.

Розроблено практичні рекомендації щодо впровадження технології централізованого зберігання паролів, налаштування політик доступу та управління ролями користувачів. Проведено тестування ефективності запропонованого рішення в умовах корпоративного середовища.

Ключові слова: кібербезпека, розмежування доступу, централізоване зберігання паролів, Passbolt, контроль доступу, захист інформації.

## SUMMARY

Malinskyi M.S. “Access control technology using a centralized password storage service”.

This master’s thesis is devoted to the research and development of an access control technology for information resources using a centralized password storage service. The paper addresses current issues of credential protection in corporate information systems and analyzes modern threats related to unauthorized access and password compromise.

The thesis analyzes modern access control models, including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), and explores approaches to centralized credential management. The architecture of a system based on the Passbolt service is described, as well as its integration with existing information systems and the cryptographic methods used to ensure data protection.

Practical recommendations for the implementation of centralized password storage technology, the configuration of access policies, and the management of user roles are developed. The effectiveness of the proposed solution is experimentally tested in a corporate environment.



Keywords: cybersecurity, access control, centralized password storage, Passbolt, information security, credential management.

| РЕЗЮМЕ (SUMMARY)<br>*до кваліфікаційної випускової роботи здобувача* | ПІБ<br>Малінський Микита Сергійович<br>Malinskyi Mykyta | | |
|---|---|---|---|
| ЗВО | Київський національний університет будівництва і архітектури | | |
| Тема *(українською та англійською)* | Технологія розмежування доступу використанням сервісу централізованого зберігання паролей<br>Access control technology using a centralized password storage service | | |
| Освітній ступінь | Магістр | | |
| Факультет | Автоматизації і інформаційний технологій | | |
| Випускова кафедра | Кібербезпеки та комп'ютерної інженерії | | |
| Спеціальність | Кібербезпека та захист інформації | | |
| Освітня програма | Безпека інформаційних і комунікаційних систем | | |
| Керівник | Шабала Є.Є. | | |
| Обсяг роботи: | *Пояснювальна записка, стор.* | *Розділів* | *Презентація, кількість слайдів* |
| | 105 | 3 | 19 |
| Розділ 1 | АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ | | |
| Розділ 2 | АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ | | |
| Розділ 3 | ПРОЕКТНА ТА ПРАКТИЧНА ЧАСТИНА | | |
| Висновки по роботі | У роботі реалізовано технологію розмежування доступу з використанням Passbolt. Проведене тестування підтвердило ефективність запропонованого рішення. | | |
| Ключові слова:<br>Keywords: | кібербезпека, розмежування доступу, централізоване зберігання паролів, Passbolt, контроль доступу, захист інформації.<br>cybersecurity, access control, centralized password storage, Passbolt, information security, credential management. | | |

Здобувач _____/ _____

Керівник _____/ _____

**ЗМІСТ**

# ВСТУП

В сучасних умовах цифровізації та інтенсивного розвитку інформаційних технологій організації дедалі більше залежать від ефективного управління доступом до своїх інформаційних ресурсів. Зростання кількості внутрішніх сервісів, розподілених команд, хмарних платформ і корпоративних додатків створює новий виклик – необхідність забезпечити безпечне, контрольоване й централізоване управління обліковими даними. Через це, формування надійної системи розмежування доступу [21, 22] стає ключовим елементом побудови комплексної інформаційної безпеки. В багатьох організаціях досі зберігаються практики використання незахищених паролів, дублювання облікових записів або передавання конфіденційних даних через ненадійні канали. У поєднанні з людським фактором це створює серйозні ризики компрометації систем, витоку інформації та порушення критично важливих бізнес-процесів. Тому, необхідність упровадження технологій централізованого зберігання паролів та побудови чіткої моделі контролю доступу є актуальним практичним завданням для сучасних організацій, особливо тих, що перебувають на етапі становлення та розвитку.

**Актуальність теми** визначається зростанням кількості кіберзагроз, спрямованих на викрадення облікових даних, а також потребою у забезпеченні прозорого контролю за діями користувачів у внутрішніх інформаційних системах. Статистика останніх років демонструє, що більшість інцидентів інформаційної безпеки пов’язана саме з неправильним управлінням доступами, використанням слабких паролів та відсутністю централізованого контролю над ними. В цьому контексті використання спеціалізованих рішень для зберігання та розподілу паролів, таких як Passbolt, дозволяє сформувати безпечну інфраструктуру, у якій доступи контролюються автоматично, а всі дії користувачів підлягають аудиту й аналізу.

**Метою дослідження** є розробка та практична реалізація технології розмежування доступу користувачів в інформаційній системі із застосуванням сервісу централізованого зберігання паролів Passbolt. Досягнення цієї мети

передбачає створення моделі, яка забезпечує безпечне керування обліковими даними, автоматизоване призначення прав доступу та контроль дій користувачів у корпоративному середовищі. В процесі дослідження розв'язуються **завдання** аналізу сучасних підходів до розмежування доступу, оцінювання технологій централізованого зберігання паролів, розробки математичної моделі доступів, проєктування архітектури вирішення та впровадження його в умовній корпоративній мережі з подальшим тестуванням і оцінкою ефективності.

**Об'єкт дослідження**: система управління доступом у корпоративних інформаційних системах.

**Предмет дослідження**: технологія розмежування доступу користувачів на основі сервісу централізованого зберігання паролів Passbolt.

**Наукова новизна роботи** полягає у розробці формалізованої моделі розмежування доступу, яка враховує поєднання ролевої структури, групових механізмів і централізованого криптографічного зберігання секретів, а також у впровадженні математичного підходу до оцінювання ефективності системи на основі критеріїв безпеки та контрольованості доступів. Крім того, новизна полягає в практичному поєднанні Passbolt з корпоративним каталогом користувачів (Active Directory / LDAP) і автоматизованою схемою призначення ролей, що дозволяє створити відтворювану модель централізованого управління доступом для невеликих і середніх організацій.

**Практичне значення роботи** полягає в тому, що результати дослідження можуть бути використані для побудови або вдосконалення систем розмежування доступу в організаціях, які потребують централізованого управління обліковими даними та контролю над їх використанням. Запропоновані моделі, алгоритми й архітектурні рішення можуть застосовуватися в корпоративних інформаційних системах, а розроблений підхід дозволяє знизити ризики витоку паролів, уникнути дублювання доступів, забезпечити прозорий аудит і сформувати єдину політику безпеки. Отримані результати можуть бути корисними як для IT-відділів і системних адміністраторів, так і для організацій, що лише формують власну інфраструктуру кібербезпеки.

**Структура роботи**: робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. В першому розділі розглядаються теоретичні засади розмежування доступу, аналізуються проблеми управління обліковими даними та наявні технології централізованого зберігання паролів, а також формулюється постановка задачі. У другому розділі здійснюється порівняльний аналіз сучасних інструментів керування паролями та детально досліджуються особливості роботи Passbolt. Третій розділ присвячений розробці та практичній реалізації моделі розмежування доступу, включаючи математичне моделювання, проєктування архітектури, інтеграцію з Active Directory / LDAP, налаштування ролей та груп і розгляд практичних кейсів. Загальний обсяг роботи – 97 сторінка.

# РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМИ ТА ПОСТАНОВКА ЗАДАЧІ

## 1.1 Поняття та значення розмежування доступу в інформаційних системах

В сучасному цифровому середовищі інформація перетворилася на один із найцінніших ресурсів організації, а її надійний захист став критично важливим завданням. Постійне зростання масштабів використання інформаційних систем у сфері бізнесу, державного управління та приватного сектору зумовлює потребу у впровадженні комплексних підходів до забезпечення інформаційної безпеки [19, 22]. Важливе місце в цій системі заходів посідає розмежування доступу до ресурсів інформаційної системи.

Під розмежуванням доступу розуміють сукупність організаційних і технічних механізмів, спрямованих на те, щоб користувачі мали доступ лише до тих даних і ресурсів, які є необхідними для виконання їхніх службових обов’язків. Цей підхід базується на принципі мінімальних привілеїв, згідно з яким кожен суб’єкт у системі повинен володіти лише мінімально необхідним рівнем доступу для виконання своїх функцій.

Відповідно до вимог міжнародного стандарту ISO/IEC 27001:2022, контроль доступу належить до базових механізмів забезпечення інформаційної безпеки. Він передбачає встановлення чітких правил, процедур і технічних засобів, що визначають, хто, за яких умов і яким способом може отримати доступ до певних інформаційних ресурсів. Згідно зі стандартами NIST SP 800-53 та ISO/IEC 27002 [35], процес контролю доступу охоплює етапи ідентифікації користувача або пристрою, перевірки достовірності їхніх облікових даних під час аутентифікації, а також авторизації, під час якої приймається рішення про надання або відмову в доступі відповідно до політик безпеки та прав користувача. Таким чином, розмежування доступу є практичною реалізацією процесу авторизації, коли на основі наперед визначених правил встановлюється рівень прав кожного суб’єкта в інформаційній системі.

В теорії та практиці інформаційної безпеки використовується декілька моделей контролю доступу, серед яких однією з найпоширеніших є модель дискреційного контролю доступу. В її межах власник ресурсу самостійно визначає, кому надавати право доступу до свого об’єкта.

1. Модель дискреційного контролю доступу (DAC – Discretionary Access Control рис. 1.1) Кожен власник ресурсу самостійно визначає, хто має право доступу до його об’єкта. Ця модель є гнучкою, однак у великих корпоративних системах може бути складною для адміністрування та створювати ризики неконтрольованого поширення доступів.

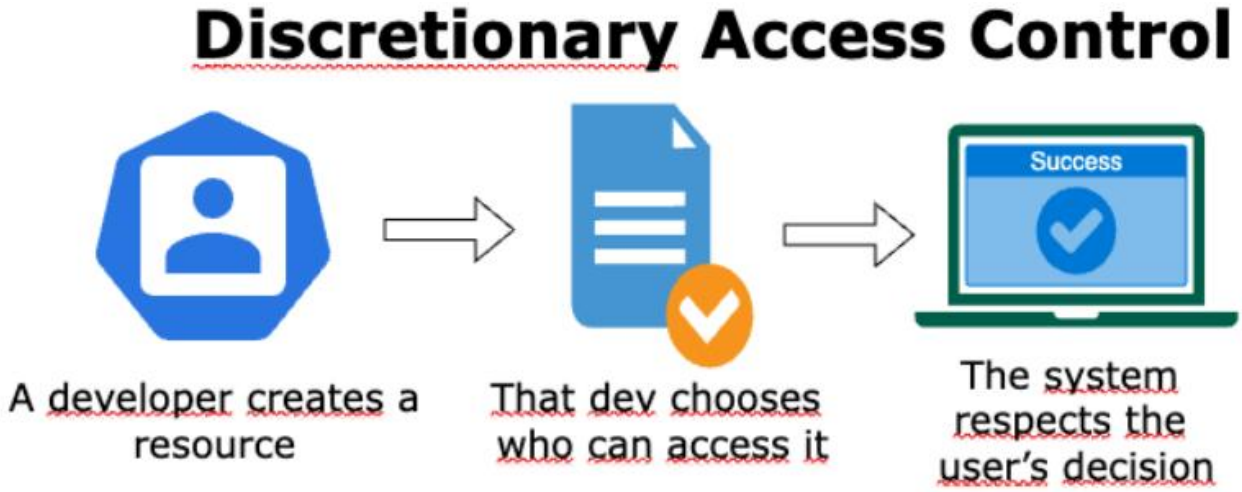



Рис. 1.1 – Модель дискреційного контролю доступу

2. Модель мандатного контролю доступу (MAC – Mandatory Access Control) Визначає рівні секретності об’єктів та допуску суб’єктів. Користувач не може самостійно змінювати права доступу. Модель часто використовується у військових і державних структурах, де критичним є дотримання політик безпеки.

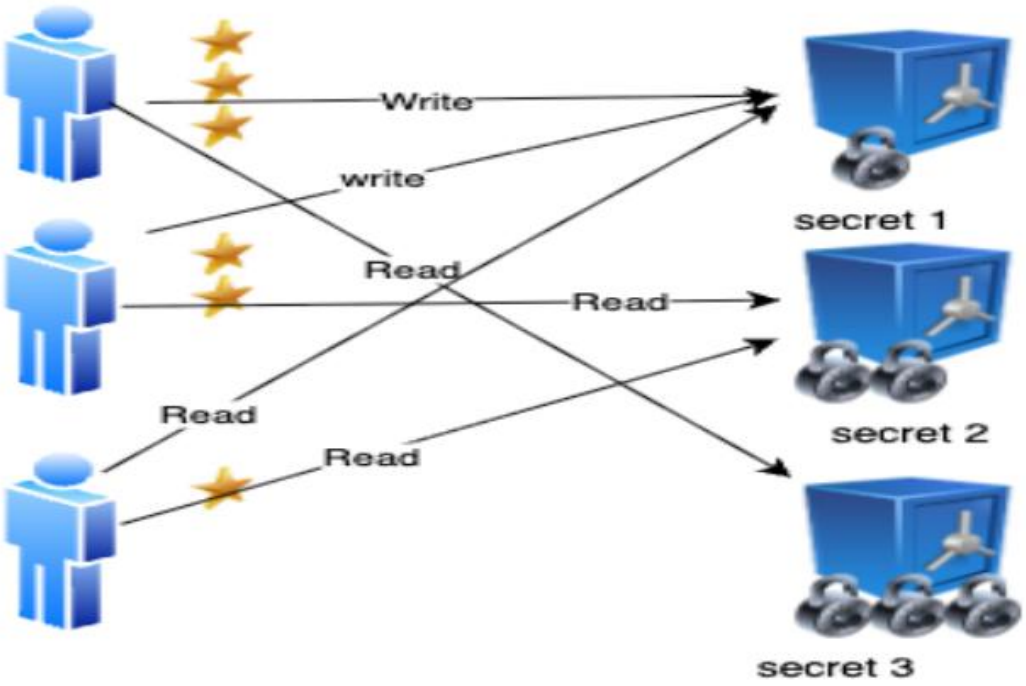



Рис. 1.2 – Модель мандатного контролю доступу

3. Модель рольового контролю доступу (RBAC – Role-Based Access Control) Найпоширеніша модель в корпоративних середовищах. Доступ визначається не конкретним користувачем, а роллю, яку він виконує. Наприклад, роль «бухгалтер» має доступ до фінансових звітів, але не до адміністративних налаштувань системи.


Рис. 1.3 – Модель рольового доступу

4. Атрибутивна модель контролю доступу (ABAC – Attribute-Based Access Control) Найсучасніший підхід, який базується на сукупності атрибутів користувача, ресурсу та контексту (час, місце, тип пристрою тощо). Дає змогу створювати гнучкі політики доступу, але потребує складних механізмів реалізації.

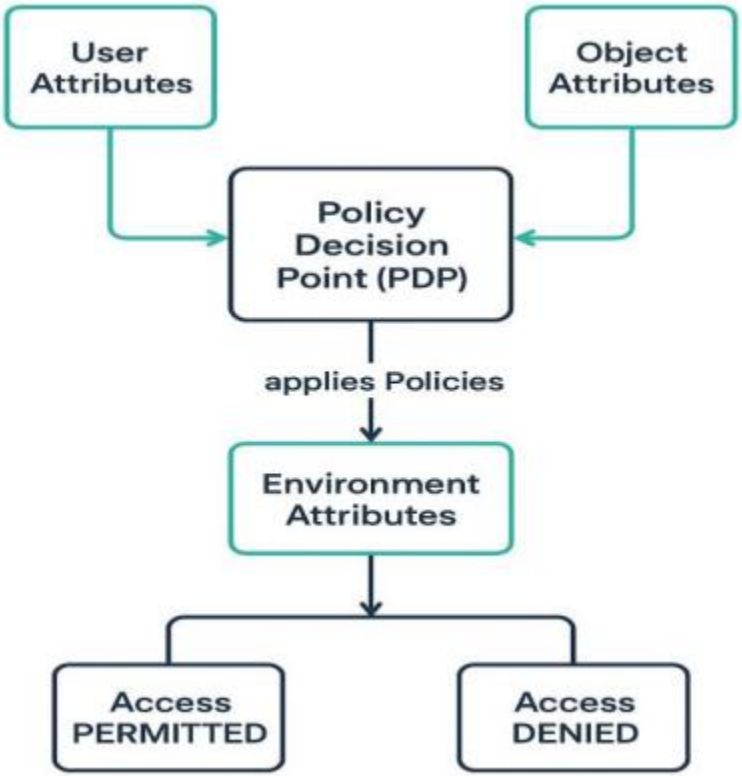



Рис. 1.4 – Модель атрибутивного контролю доступу

Вибір моделі залежить від розміру організації, типу інформаційних ресурсів та рівня вимог до безпеки.

Щодо розмежування, то в сучасних організаціях розмежування доступу відіграє ключову роль у побудові надійної системи інформаційної безпеки, адже саме від коректного управління правами користувачів залежить збереження даних, стабільність бізнес-процесів та довіра до цифрових ресурсів. Ефективно вибудувана система контролю доступу одночасно забезпечує захист конфіденційної інформації від несанкціонованого ознайомлення, підтримує цілісність даних, запобігаючи як випадковим, так і навмисним змінам, а також підвищує підзвітність користувачів, оскільки всі дії в системі виконуються під конкретними обліковими записами. Важливим результатом її впровадження є і

зниження ризиків внутрішніх загроз, які найчастіше виникають саме через надання надмірних прав доступу.

Ігнорування принципів розмежування доступу призводить до значного зростання кіберризиків. За статистикою світових інцидентів, понад шістдесят відсотків випадків витоку інформації пов’язані з неправильним або надмірним налаштуванням прав користувачів. Подібні порушення здатні спричинити серйозні фінансові збитки, втрату ділової репутації, а також невідповідність вимогам нормативно-правових актів і міжнародних стандартів, зокрема GDPR, ISO 27001, HIPAA [13] та інших.

Технічна реалізація розмежування доступу здійснюється на кількох рівнях [15]. На мережевому рівні для цього використовуються міжмережеві екрани, віртуальні приватні мережі та технології сегментації мережі на основі VLAN. На рівні операційних систем контроль доступу забезпечується механізмами облікових записів, груп користувачів і системними політиками безпеки. Прикладний рівень реалізується через ролі та політики доступу в програмних продуктах, базах даних і веб-додатках, тоді як фізичний рівень включає контролери доступу, електронні ключі та системи відеоспостереження. В корпоративних інформаційних системах всі ці рівні взаємодіють між собою, формуючи багаторівневу й комплексну систему захисту.

Отже, розмежування доступу є фундаментальним елементом сучасної системи інформаційної безпеки. Воно не лише обмежує можливості зловмисників, а й забезпечує прозорість та контроль дій користувачів у межах інформаційних систем. Використання сучасних моделей контролю доступу, зокрема RBAC та ABAC, в поєднанні з системами управління ідентичностями є необхідною умовою безпечного та стабільного функціонування організацій у цифровому середовищі.

## 1.2 Проблеми управління обліковими даними у сучасних організаціях

Однією з ключових складових забезпечення інформаційної безпеки є ефективне управління обліковими даними користувачів. В міру стрімкого

зростання кількості інформаційних систем, хмарних сервісів, внутрішніх і зовнішніх ресурсів невпинно збільшується й кількість облікових записів, які потребують постійного контролю [20, 23]. Неефективне керування цими даними створює суттєві загрози для безпеки, стабільності роботи та репутації організації.

Під обліковими даними розуміють сукупність ідентифікаційних елементів, які використовуються для встановлення особи користувача в системі, підтвердження його прав і надання доступу до інформаційних ресурсів. Найпоширенішим варіантом є поєднання логіна та пароля, проте дедалі частіше застосовуються також токени, цифрові сертифікати, біометричні параметри та механізми багатофакторної аутентифікації. Управління обліковими даними, відоме як Identity and Access Management (IAM), являє собою комплекс політик, процесів і технологій, спрямованих на правильне створення, використання, зберігання та видалення облікових записів. Відповідно до стандарту ISO/IEC 24760-1:2019, система IAM охоплює ідентифікацію суб’єктів, управління їхніми атрибутами, надання прав доступу та контроль за використанням цифрових ідентичностей.

Із розвитком цифрової інфраструктури та активним переходом бізнесу до хмарних технологій процес управління обліковими даними стає дедалі складнішим. Однією з основних проблем є стрімке зростання кількості облікових записів, що значно ускладнює їх адміністрування та контроль. Серйозну загрозу становить і повторне використання паролів у кількох системах, адже компрометація одного ресурсу може відкрити зловмисникам доступ до інших внутрішніх сервісів організації. Не менш небезпечним є використання слабких або передбачуваних паролів, оскільки велика частина інцидентів із зламом облікових записів спричиняється саме такими порушеннями корпоративної політики безпеки.

Окрему категорію ризиків становлять фішингові атаки та методи соціальної інженерії, за допомогою яких зловмисники отримують доступ до конфіденційних даних користувачів. Попри наявність сучасних технічних засобів захисту, людський фактор залишається найуразливішою ланкою системи безпеки [24].

Ускладнює ситуацію й відсутність єдиної системи автентифікації та авторизації, що призводить до дублювання облікових записів, неузгодженості політик доступу та помилок під час надання прав користувачам. Це, своєю чергою, суттєво ускладнює аудит і моніторинг.

Ще однією поширеною проблемою є недостатній контроль за життєвим циклом облікових записів. В багатьох організаціях після звільнення працівників або зміни їхніх посад облікові записи залишаються активними, що створює реальні загрози несанкціонованого доступу, особливо у великих компаніях із розгалуженою IT-інфраструктурою. Водночас, відсутність централізованої системи управління призводить до того, що різні інформаційні системи функціонують незалежно, а адміністраторам доводиться вручну синхронізувати облікові записи, що знижує ефективність управління та підвищує ймовірність помилок.

Неналежне управління обліковими даними безпосередньо впливає на рівень кібербезпеки організації та може призводити до серйозних негативних наслідків. Одним із найбільш небезпечних ризиків є компрометація критично важливих систем у результаті використання викрадених або вразливих облікових записів. Це, своєю чергою, часто спричиняє витік персональних і корпоративних даних, що може порушувати вимоги чинного законодавства, зокрема положення GDPR [27]. Подібні інциденти неминуче призводять до втрати довіри з боку клієнтів і партнерів, а також до значних фінансових збитків, пов’язаних з ліквідацією наслідків атак, відновленням працездатності систем і сплатою штрафів регуляторним органам. Дані звітів Verizon Data Breach Investigations Report свідчать, що облікові дані залишаються одним із найпопулярніших об’єктів кібератак, а більш ніж у половині випадків компрометації корпоративних систем зловмисники спочатку отримують або підбирають саме облікові записи користувачів.

З метою зниження зазначених ризиків сучасні організації впроваджують комплекс технічних і організаційних рішень. Поширеним підходом є використання систем єдиного входу, які дозволяють користувачеві проходити

автентифікацію лише один раз і отримувати доступ до всіх корпоративних ресурсів, що спрощує адміністрування та підвищує рівень безпеки завдяки централізованому контролю. Важливу роль відіграє і багатофакторна автентифікація, яка поєднує кілька факторів підтвердження особи та значно ускладнює компрометацію облікових записів. Додатковий захист забезпечують політики складності та регулярної зміни паролів, які знижують імовірність їх підбору. Широко застосовуються також централізовані системи управління ідентичностями, зокрема Azure AD, Okta, Keycloak і FreeIPA [26, 28], що дають змогу автоматизувати створення, оновлення та видалення облікових записів і керувати доступом на основі ролей або атрибутів. Водночас важливе значення має й постійне навчання персоналу, адже регулярні тренінги з кібергігієни суттєво зменшують кількість інцидентів, спричинених людським фактором.

Попри розвиток сучасних технологій захисту, саме людський фактор залишається однією з головних причин інцидентів інформаційної безпеки. Працівники нерідко зберігають паролі в незахищених місцях, передають їх колегам або користуються спільними обліковими записами. За відсутності належного контролю такі дії можуть мати критичні наслідки навіть за умови використання сучасних технічних засобів захисту. Тому, для мінімізації ризиків необхідно розробляти чіткі організаційні політики управління обліковими даними, які регламентують порядок створення, використання, передачі та видалення облікових записів. Подібні політики мають бути невід’ємною складовою системи управління інформаційною безпекою організації.

Отже, проблеми управління обліковими даними в сучасних організаціях мають комплексний характер і охоплюють як технічні, так і організаційні аспекти. Зростання кількості цифрових сервісів, розширення можливостей віддаленого доступу та поява нових форм кібератак вимагають системного підходу до захисту ідентичностей користувачів. Ефективне управління обліковими записами має базуватися на принципах мінімальних привілеїв, централізованого контролю, використанні багатофакторної автентифікації та постійному моніторингу подій безпеки. Впровадження систем IAM і рішень для безпечного зберігання паролів є

важливим напрямом розвитку корпоративної кібербезпеки, що дозволяє досягти балансу між зручністю для користувачів і високим рівнем захисту інформаційних ресурсів.

### 1.3 Огляд технологій централізованого зберігання паролів

Із поступом цифрової епохи та все ширшим уживанням інформаційних мереж, проблема надійного забезпечення конфіденційності логінів та паролів стала надзвичайно важливою. Сучасні компанії, як правило, оперують великою кількістю (десятки чи навіть сотні) різнорідних платформ, сервісів та програм, які вимагають підтвердження особи користувачів. Коли немає дієвого інструменту для єдиного контролю над обліковими даними, виникає безлад у їх зберіганні, надмірне дублювання та, як наслідок, зростає небезпека несанкціонованого доступу. Централізоване зберігання паролів – це технічне рішення, що полягає в застосуванні виділеної платформи чи послуги для надійного утримання, адміністрування та спільного доступу до реєстраційних даних в межах компанії. Ці системи втілюють ідею створення «єдиного надійного сейфу» (vault), де всі секретні комбінації тримаються у зашифрованому стані, а перегляд їх регулюється правилами безпеки, моделями ролей та криптографічними методами.

**Основні завдання централізованого зберігання паролів**:

1. Захист облікових даних – всі паролі зберігаються у зашифрованому вигляді з використанням сучасних криптографічних алгоритмів (AES-256, RSA, Argon2 тощо).

2. Контроль доступу – визначення, хто і до яких паролів має доступ, із можливістю обмеження дій (читання, редагування, спільне використання).

3. Аудит і моніторинг – ведення журналів дій користувачів, фіксація змін, перевірка використання облікових даних.

4. Автоматизація – інтеграція з корпоративними системами (Active Directory, LDAP, SSO), автоматичне оновлення паролів, виявлення слабких, або скомпрометованих облікових даних.

5. Спільна робота – безпечне надання доступу членам команди без передачі паролів у відкритому вигляді.

Залежно від архітектури, цільової аудиторії та принципів роботи системи централізованого зберігання паролів можна умовно поділити на кілька типів:

**Хмарні сервіси (SaaS-рішення)**:

Такі системи надаються як онлайн-сервіси, що зберігають паролі у хмарному сховищі. Вони не потребують власної інфраструктури та дозволяють швидко розгорнути рішення без складних налаштувань.

Приклади:

- 1Password – корпоративний менеджер паролів з підтримкою спільних сейфів, багатофакторної автентифікації, SSO та інтеграцією з Azure AD.
- LastPass – один з найпопулярніших SaaS-парольних менеджерів [4, 5], який підтримує синхронізацію між пристроями, автозаповнення та централізоване керування командами
- Dashlane – пропонує гнучкі корпоративні плани з аналітикою безпеки, виявленням витоків і інтеграцією з браузерами.

Таблиця 1.1

**Переваги та недоліки хмарних сервісів**

| Переваги | Недоліки |
|---|---|
| Швидке розгортання | Залежність від хмарної інфраструктури стороннього постачальника |
| Зручність користування | Потенційні ризики компрометації у випадку зламу сервісу |
| Оновлення та підтримка з боку постачальника | Відсутність повного контролю над даними |

**Локальні серверні рішення (On-Premise)**

Це рішення розгортаються у внутрішній інфраструктурі організації, забезпечуючи повний контроль над системою та збереженням даних.

Приклади:

— Passbolt – open-source система для спільного зберігання паролів [6, 7, 9, 10] у командах, з підтримкою GPG-шифрування, групового доступу та вебінтерфейсу.

— Bitwarden Server – корпоративна версія популярного менеджера Bitwarden [12], що дозволяє самостійне хостування.

— KeePass / KeePassXC – настільні застосунки з підтримкою шифрування AES та можливістю спільного використання бази через файлові сховища.

Таблиця 1.2

**Переваги та недоліки серверних рішень**

| **Переваги** | **Недоліки** |
|---|---|
| Повний контроль над інфраструктурою | Складність розгортання та адміністрування |
| Можливість інтеграції з внутрішніми системами (LDAP, Kerberos, VPN) | Потреба у технічному персоналі |
| Більша гнучкість у налаштуваннях політик безпеки | Обмежена масштабованість без додаткових ресурсів |

**Гібридні рішення**

Поєднують переваги хмарних і локальних систем. Ключі шифрування зберігаються на стороні клієнта, а паролі – в хмарному сховищі або внутрішній бази даних.

Приклади:

— Keeper Security Enterprise – підтримує локальне керування ключами, інтеграцію з SIEM та можливість вибору місця зберігання даних.

— Zoho Vault – забезпечує централізоване зберігання паролів у хмарі з можливістю локальної автентифікації.

Таблиця 1.3

**Порівняння хмарних, локальних та гібридних рішень**

| **Критерій** | **Хмарні рішення** | **Локальні рішення** | **Гібридні рішення** |
|---|---|---|---|
| **Контроль над даними** | Обмежений | Повний | Гнучкий |
| **Витрати на розгортання** | Низькі | Високі | Середні |
| **Безпека** | Залежить від постачальника | Повна відповідальність організації | Баланс |
| **Масштабованість** | Висока | Обмежена | Висока |
| **Автоматизація** | Вбудована | Налаштовується вручну | Частково вбудована |
| **Приклади** | LastPass, Dashlane | Passbolt, KeePass | Keeper, Zoho Vault |

Сучасні технології зберігання паролів активно розвиваються відповідно до зростаючих вимог безпеки та зручності користування. Однією з провідних тенденцій є перехід до архітектури Zero-Knowledge, за якої навіть постачальник сервісу не має доступу до зашифрованих даних користувача, що суттєво підвищує рівень конфіденційності. Широкого поширення набуває використання апаратних модулів безпеки, зокрема HSM і TPM, для надійного зберігання криптографічних ключів. Важливим напрямом розвитку є інтеграція менеджерів паролів із технологіями єдиного входу SSO, що дозволяє значно зменшити кількість паролів, які користувачеві необхідно запам’ятовувати. Також активно впроваджується підтримка стандартів FIDO2 і WebAuthn, які відкривають можливості для безпарольної автентифікації. Окрему роль відіграє застосування штучного інтелекту для аналізу рівня захищеності паролів, зокрема для виявлення слабких, повторюваних або потенційно скомпрометованих облікових даних.

Отже, технології централізованого зберігання паролів [4, 5, 25] сьогодні є невід'ємною складовою сучасної системи кібербезпеки. Вони дають змогу організаціям суттєво знизити ризики, пов'язані з людським фактором, уніфікувати політики безпеки та підвищити рівень керованості інформаційною інфраструктурою. Особливе місце серед таких рішень посідають open-source системи, зокрема Passbolt, які поєднують у собі прозорість, гнучкість і можливість адаптації до конкретних потреб організації. У наступних розділах буде розглянуто архітектуру та принципи роботи Passbolt, а також проведено практичну оцінку ефективності його використання в корпоративному середовищі.

### 1.4. Роль опенсорсних рішень у забезпеченні кібербезпеки організацій

В сучасних умовах стрімкої цифровізації та зростання кіберзагроз вибір програмного забезпечення для створення надійної системи кібербезпеки набуває стратегічного значення. Все частіше організації віддають перевагу open-source рішенням, які дозволяють не лише знизити витрати, а й підвищити прозорість, керованість і рівень довіри до систем захисту.

Open-source програмне забезпечення представляє собою програми з відкритим вихідним кодом, доступним для перегляду, аналізу, модифікацій та розповсюдження. Такий спосіб суттєво відрізняється від закритих, або пропрієтарних систем, де код є власністю розробника і недоступний для зовнішнього аудиту.

Однією з ключових переваг open-source є прозорість, що формує високий рівень довіри до програмного забезпечення. Будь-який кваліфікований спеціаліст або незалежна організація може ретельно дослідити код, переконатися у відсутності шкідливих вставок чи прихованих функцій для збору даних. На відміну від комерційних продуктів, де перевірка кодової бази можлива лише за згодою розробника, відкритий код дозволяє будь-якому експерту виявляти і усувати потенційні вразливості [13, 22], що підвищує безпеку системи і сприяє

спільному вдосконаленню програмного забезпечення за участю зацікавленої спільноти.

Гнучкість і адаптивність, теж, роблять open-source рішення привабливими. Організації можуть модифікувати конфігурації, архітектуру та політики доступу відповідно до власних потреб без обмежень ліцензій. Наприклад, у корпоративному середовищі open-source системи управління паролями, такі як Passbolt або Bitwarden, легко інтегруються з внутрішніми LDAP чи Active Directory без потреби купувати додаткові модулі. Відкритий код дозволяє створювати власні розширення, автоматизувати процеси та інтегрувати безпекові рішення у внутрішню інфраструктуру, забезпечуючи повну відповідність політикам організації.

Економічна ефективність є ще однією перевагою. Open-source продукти зазвичай не потребують значних витрат на придбання або коштують значно дешевше порівняно з пропрієтарними аналогами. Основні фінансові витрати стосуються лише інсталяції, адміністрування та обслуговування, що в кінцевому підсумку обходиться дешевше за регулярні ліцензійні відрахування. Крім того, більшість open-source рішень підтримується розгалуженими спільнотами користувачів, що забезпечує технічну допомогу, фахові поради та доступ до оновлень без додаткових витрат і необхідності укладати договір із комерційним розробником.

Щодо прив’язки до конкретного вендора, воно є однією з основних проблем використання пропрієтарних комерційних рішень. В таких випадках організація втрачає можливість самостійно змінювати налаштування програмного забезпечення або переходити на інші продукти без значних фінансових витрат і технічних складнощів.

Рішення з відкритим кодом усувають цю залежність, надаючи повний контроль над системою. Організація може розгортати її на власних обчислювальних потужностях, адаптувати до специфічних вимог та переносити на інші технічні бази без будь-яких перешкод. Це забезпечує автономність та

стійкість IT-середовища, що особливо важливо для державних установ, оборонно-промислового комплексу та великих корпоративних структур.

Ще однією перевагою є оперативніше впровадження змін і усунення вразливостей. Завдяки широкій спільноті фахівців і аналітиків, які працюють над open-source продуктами, патчі безпеки виходять значно швидше, а дефекти та потенційні загрози усуваються у публічному полі, без необхідності чекати на офіційне оновлення від виробника. Приклади таких рішень, як OpenSSL, Linux, ClamAV, Suricata, pfSense, Passbolt [33, 35] і Bitwarden, демонструють, що навіть великі комерційні гравці використовують відкриті системи як основу для створення власних засобів кіберзахисту.

Попри численні переваги, open-source рішення мають і певні виклики, які слід враховувати при їх впровадженні. Одним із них є відсутність офіційної гарантії підтримки – не всі проєкти активно розвиваються, тому організація має самостійно забезпечувати технічну підтримку. Використання таких рішень вимагає високої кваліфікації персоналу, оскільки для налаштування, аудиту коду та інтеграції потрібні спеціалісти з глибокими знаннями систем безпеки. Іноді виникають проблеми з відповідністю стандартам, оскільки не всі open-source продукти сертифіковані за галузевими, або державними нормами, такими як ISO/IEC 15408 [13] або Common Criteria. Також, слід враховувати фрагментованість інструментів – велика кількість незалежних розробників ускладнює забезпечення повної сумісності між різними компонентами.

Але, більшість цих ризиків можна знизити за рахунок правильного підходу до вибору рішень, регулярного аудиту та участі у спільноті проєкту.

Таблиця 1.4

**Приклади опенсорсних рішень у сфері кібербезпеки**

| **Напрямок** | **Open-source рішення** | **Призначення** |
|---|---|---|
| **Управління паролями** | Passbolt, Bitwarden, KeePassXC | Централізоване зберігання та спільне використання паролів |

Продовження таблиця 1.4

| | | |
|---|---|---|
| **Мережевий захист** | pfSense, OPNsense, Suricata, Snort | Мережеві екрани, IDS/IPS системи |
| **Захист кінцевих точок** | ClamAV, OSSEC, Wazuh | Антивірусний і поведінковий моніторинг |
| **Криптографія** | OpenSSL, GnuPG | Шифрування даних, управління ключами |
| **Аналіз безпеки** | Metasploit, OpenVAS | Тестування на проникнення, сканування вразливостей |
| **Логування та моніторинг** | ELK Stack, Graylog | Централізований збір і аналіз журналів подій |

Впровадження програмного забезпечення з відкритим кодом змінює не лише технологічну інфраструктуру організації, а й підхід до кібербезпеки в цілому. Відкриті розробки стимулюють обмін досвідом, спільну роботу та постійне вдосконалення процесів. Організації, які активно інтегрують open-source рішення, зазвичай формують команди кібербезпеки з мисленням, орієнтованим на прозорість, ясність і уніфікацію робочих процедур.

Крім того, використання open-source підтримує незалежність у сфері кібербезпеки, надаючи державним та комерційним структурам можливість створювати власні продукти на основі відкритих технологічних платформ, уникаючи залежності від зовнішніх постачальників та закритих систем.

Отже, програмне забезпечення з відкритим кодом відіграє ключову роль в формуванні сучасної архітектури захисту інформації, забезпечуючи прозорість процесів, повний контроль і оптимізацію витрат. Завдяки таким інструментам організації можуть розробляти власні стратегії безпеки без комерційної залежності, зберігаючи високий рівень якості та стійкості захисту. Особливу увагу варто приділяти незалежним розробкам при впровадженні ефективних механізмів контролю доступу та автентифікації, де яскравим прикладом успішного підходу є Passbolt.

## 1.5. Постановка задачі дослідження

Проведений аналіз теоретичних аспектів розмежування доступу, проблем управління обліковими даними, сучасних технологій централізованого зберігання паролів та ролі open-source рішень в кібербезпеці дозволяє визначити основну науково-практичну задачу цієї магістерської роботи.

Сучасні організації стикаються з проблемами неефективного управління обліковими даними та недостатньо контрольованого доступу до ресурсів інформаційної системи. Паролі часто зберігаються у незахищеному вигляді – у текстових файлах, браузерах або приватних повідомленнях, що створює високі ризики витоку конфіденційної інформації. Відсутність централізованого контролю доступу ускладнює аудит дій користувачів, підвищує ймовірність внутрішніх загроз та унеможливлює формування єдиної політики безпеки.

З урахуванням цього основною проблемою, яку потрібно вирішити в рамках дослідження, є розробка та впровадження технології розмежування доступу на основі сервісу централізованого зберігання паролів, що забезпечить підвищення рівня інформаційної безпеки в організації.

Метою магістерської роботи є розробка та практична реалізація технології розмежування доступу користувачів в інформаційній системі з використанням сервісу централізованого зберігання паролів Passbolt. Досягнення цієї мети передбачає створення моделі, яка дозволить забезпечити безпечне зберігання облікових даних, їх централізоване адміністрування та контроль за доступом до інформаційних ресурсів.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

1. Проаналізувати існуючі підходи до розмежування доступу в інформаційних системах та визначити їхні переваги й недоліки.

2. Дослідити сучасні технології та інструменти централізованого зберігання паролів, оцінити їхню ефективність і можливість інтеграції в корпоративне середовище.

3. Визначити вимоги до системи управління обліковими даними та критерії її безпеки.

4. Розробити архітектурну модель розмежування доступу на основі open-source сервісу Passbolt.

5. Реалізувати впровадження системи Passbolt у корпоративній мережі (на прикладі умовної організації) з урахуванням ролей, груп користувачів і рівнів доступу.

6. Провести тестування системи, оцінити ефективність та стійкість до можливих кіберзагроз.

7. Надати рекомендації щодо оптимізації процесів управління доступом і підвищення рівня захисту інформації в організаціях.

Об’єктом дослідження є система управління доступом у корпоративних інформаційних системах, тоді як предметом дослідження виступає технологія розмежування доступу на основі централізованого зберігання паролів із використанням open-source рішення Passbolt.

В роботі застосовуються різні методи дослідження. Аналітичний підхід використовується для вивчення існуючих систем керування доступом та менеджерів паролів, порівняльний – для оцінки ефективності різних підходів до зберігання облікових даних. Моделювання допомагає побудувати архітектуру системи розмежування доступу, а експериментальний метод застосовується для тестування впровадженої системи у реальних умовах. Системний аналіз дозволяє узагальнити результати та розробити рекомендації щодо подальшого удосконалення технологій безпеки.

Очікувані результати роботи передбачають розробку концепції та моделі розмежування доступу з використанням централізованого сховища паролів, реалізацію прототипу системи на базі Passbolt і проведення її тестування, оцінку підвищення рівня інформаційної безпеки після впровадження технології та формування практичних рекомендацій щодо застосування open-source рішень у корпоративному середовищі.

Загалом, постановка задачі дослідження визначає подальшу структуру магістерської роботи, формуючи логічний зв’язок між теоретичною частиною, аналізом існуючих рішень і розробкою власної моделі розмежування доступу. Від коректного формулювання проблеми залежить не лише послідовність викладення матеріалу, а й можливість отримати об’єктивні, вимірювані та практично значущі результати. В межах цього дослідження ключовою метою є з’ясування того, наскільки ефективно open-source системи централізованого зберігання паролів можуть виконувати роль базового компонента комплексної моделі управління доступами, та чи справді вони здатні забезпечити належний рівень безпеки для корпоративних середовищ різного масштабу.

Отримані результати дозволять не лише оцінити функціональні можливості таких рішень, а й виявити їхні сильні та слабкі сторони у практичному застосуванні. Особливо важливо проаналізувати, як саме подібні системи взаємодіють з існуючою інфраструктурою організації, наскільки добре масштабуються разом із зростанням штату та чи можуть забезпечити стабільність і керованість доступів у довгостроковій перспективі. Такий спосіб дасть змогу сформувати цілісне бачення того, як open-source інструменти впливають на побудову безпечних внутрішніх процесів, зменшують кількість ручних операцій та сприяють підвищенню прозорості в управлінні правами користувачів.

# РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ТА ІНСТРУМЕНТІВ

## 2.1. Підходи до управління обліковими даними в сучасних інформаційних системах

В умовах сьогоденних підприємств надійність захисту інформації надзвичайно вагомо корелює із якістю керування акаунтами користувачів. Оскільки кількість внутрішніх сервісів, хмарних програм, віртуальних платформ та можливостей для дистанційної праці невпинно примножується, це значно обтяжує процедури підтвердження особи (автентифікації), надання дозволів (авторизації) та регулювання доступу. Відтак, управління обліковими даними перетворилося на один із ключових векторів еволюції архітектур кіберзахисту.

Облікові дані (креденшелс) – це сукупність відомостей, що застосовуються з метою підтвердження ідентичності як індивіда, так і програмного сервісу. Хоча найпоширенішим методом верифікації особи досі виступає пара логін/пароль, технологічний прогрес стимулює активніше впровадження багатофакторної перевірки (MFA), динамічних одноразових кодів, цифрових сертифікатів та біометричних ознак.

Внаслідок розширення парку систем та сервісів, адміністрування паролів набуває все більшої заплутаності: користувачі нерідко застосовують ідентичні набори даних для входу в різні ресурси, ігноруючи необхідні стандарти безпеки. Це відкриває лазівки у захисті, якими зацікавлені зловмисники. Для подолання цих труднощів було випрацьовано низку методологій для консолідованого керування та моніторингу доступу, серед яких лідерські позиції займають системи IAM (Управління ідентифікацією та доступом), PAM (Управління привілейованим доступом), SSO (Єдиний вхід) та сховища паролів (Password Vaults).

**Система управління ідентифікацією та доступом (IAM)**

Identity and Access Management (IAM) – це комплексна концепція, що поєднує політики [23, 31], процеси та технології для управління цифровими

ідентичностями користувачів та їхніми правами доступу до ресурсів. IAMрішення дозволяють централізовано створювати, змінювати та видаляти облікові записи користувачів, а також контролювати їхні привілеї відповідно до ролі в організації.

Основні компоненти системи IAM:

— Ідентифікація користувачів – створення унікальних записів у системі
— Автентифікація – перевірка достовірності особи (паролі, токени, біометрія) [17]
— Авторизація – визначення рівня доступу
— Аудит – реєстрація дій користувачів і контроль дотримання політик. IAM забезпечує впровадження принципу «єдиного джерела істини» (single source of truth), коли дані про користувачів зберігаються централізовано, що спрощує управління доступом у великих організаціях.

Приклади IAM-рішень:

— Microsoft Entra ID (раніше Azure AD)
— Okta Identity Cloud
— Keycloak (open-source)
— ForgeRock Identity Platform

Перевагою IAM є комплексність: вона об’єднує всі аспекти управління користувачами, проте її впровадження потребує значних ресурсів і підготовки.

**Управління привілейованим доступом (PAM)**

Privileged Access Management (PAM) – це підхід, спрямований на захист облікових даних користувачів із підвищеними правами (адміністраторів, розробників, системних інженерів) [29, 30]. Ці облікові записи мають доступ до критичних систем, серверів і конфіденційної інформації, тому є особливо цінною ціллю для кіберзлочинців.

PAM-рішення реалізують такі функції:

— зберігання привілейованих паролів у зашифрованому сховищі (vault)

— автоматичну ротацію паролів і ключів доступу

— моніторинг та запис сесій адміністраторів

— виявлення і блокування аномальних дій

Типовий сценарій: адміністратор не знає пароля до сервера – система PAM надає тимчасовий доступ, зберігаючи всі дії в журналі аудиту.

Приклади рішень PAM:

— CyberArk

— BeyondTrust

— Thycotic Secret Server

— HashiCorp Vault (open-source)

Таким чином, PAM є спеціалізованим інструментом, орієнтованим на контроль критично важливих доступів, тоді як IAM вирішує ширше коло завдань управління користувачами. Єдиний вхід у систему (SSO)

Single Sign-On (SSO) – це технологія, що дозволяє користувачу проходити автентифікацію один раз і отримувати доступ до кількох систем або додатків без повторного введення облікових даних. SSO базується на довірених зв’язках між системами і реалізується через протоколи SAML, OAuth 2.0, OpenID Connect. Основна ідея полягає в тому, що користувач автентифікується в єдиній системі (наприклад, корпоративному домені, або хмарному сервісі), після чого отримує токен доступу, який автоматично використовується для входу до інших систем.

Таблиця 2.1

**Порівняння SSO**

| **Переваги** | **Недоліки** |
|---|---|
| Зменшення кількості паролів, які потрібно запам'ятовувати | У разі компрометації головного облікового запису зловмисник отримує доступ до всіх систем |

Продовження таблиці 2.1

| | |
|---|---|
| Підвищення безпеки завдяки централізованому контролю автентифікації | Складність налаштування між різними платформами |
| Покращення зручності користувачів | — |

Приклади впровадження систем єдиного входу включають Microsoft Entra SSO, Google Identity Platform, Keycloak, Okta та Auth0. Хоча SSO не замінює менеджери паролів, воно значно зменшує кількість облікових даних, якими користувачеві доводиться оперувати.

Системи централізованого зберігання паролів, або Password Vaults [4, 5, 25], призначені для безпечного зберігання, генерації та спільного використання паролів. Вони створюють зашифроване сховище, доступ до якого контролюється єдиним головним ключем (master password) або багатофакторною автентифікацією. На відміну від систем управління ідентичностями (IAM) чи привілеями (PAM), менеджери паролів мають більш вузьку спеціалізацію – безпечне зберігання та розподіл облікових даних між користувачами. Такі рішення особливо корисні для малих і середніх компаній, де повноцінне впровадження IAM/PAM може бути економічно недоцільним.

Сучасні системи централізованого зберігання паролів забезпечують генерацію складних паролів, централізоване шифроване зберігання (AES-256, GPG, Argon2), спільний доступ для груп користувачів, аудит змін та дій, автоматичне заповнення форм автентифікації, а також інтеграцію з LDAP, або Active Directory. Типовими прикладами таких рішень є Passbolt, що підтримує GPG-шифрування та командну роботу [7, 9, 10]; Bitwarden із мультиплатформенною підтримкою; KeePass та KeePassXC для офлайн-зберігання бази; LastPass як хмарне рішення для бізнесу; 1Password із корпоративними сейфами та багатофакторною автентифікацією.

Таблиця 2.2

**Порівняння підходів IAM, PAM, SSO та Password Vault**

| **Підхід** | **Основна мета** | **Рівень складності** | **Приклади рішень** | **Орієнтація** |
|---|---|---|---|---|
| **IAM** | **Централізоване управління ідентичностями та доступом** | Високий | Azure AD, Okta, Keycloak | Великі корпорації |
| **PAM** | **Контроль привілейованих облікових записів** | Високий | CyberArk, BeyondTrust, Vault | IT-відділи, DevOps |
| **SSO** | **Єдиний вхід у кілька систем** | Середній | Auth0, Keycloak, Okta | Користувачі |
| **Password Vault** | **Безпечне зберігання та обмін паролями** | Низький/середній | Passbolt, Bitwarden, KeePass | Будь-які організації |

Управління обліковими даними є ключовим елементом інформаційної безпеки, і кожен із розглянутих підходів вирішує певну частину цієї проблеми. Системи IAM забезпечують комплексне керування ідентичностями, PAM контролює доступ адміністративного рівня, SSO підвищує зручність користувача та зменшує кількість паролів, а Password Vault гарантує безпечне централізоване зберігання облікових даних.

Для організацій, які перебувають на етапі становлення або мають обмежені ресурси, найбільш доцільним є впровадження open-source Password Vault системи, наприклад Passbolt, що дозволяє забезпечити централізований контроль доступу без значних фінансових витрат.

## 2.2. Критерії вибору системи керування паролями для організацій на етапі становлення

Під час формування інформаційної інфраструктури молодих організацій одним із ключових завдань є створення надійної та ефективної системи керування обліковими даними. На цьому етапі компанії часто мають обмежені фінансові та кадрові ресурси, тому вибір системи має базуватися не лише на її функціональних можливостях, а й на економічній доцільності та масштабованості рішення.

Для об'єктивного визначення оптимального програмного забезпечення доцільно застосовувати методи багатокритеріального аналізу (Multi-Criteria Decision Making, MCDM), що дозволяють оцінювати альтернативи за сукупністю критеріїв із урахуванням їхньої відносної важливості.

В межах цього дослідження визначено п'ять основних критеріїв, які впливають на доцільність впровадження системи керування паролями для молодих організацій. Перший критерій – рівень безпеки, що оцінюється за ступенем захисту даних, типом шифрування, підтримкою багатофакторної автентифікації, політиками доступу та аудитом дій. Другий критерій – вартість впровадження, яка включає фінансові витрати на ліцензії, розгортання та обслуговування. Третій – зручність використання, що визначається простотою інтерфейсу, швидкістю доступу та навчанням персоналу. Четвертий критерій – масштабованість, тобто, можливість розширення системи відповідно до росту організації. П'ятий критерій – відкритість коду, що передбачає наявність open-source ліцензії, можливість аудиту та кастомізації.

Для кількісного порівняння систем вводиться оцінкова функція ефективності (E), яка враховує вагові коефіцієнти важливості кожного з критеріїв:

$$E_i = \sum_{i=1}^{n} w_i \cdot k_{ij} \qquad (2.1)$$

де:

— $E_i$ — інтегральна оцінка ефективності i-ї системи,

— $w_j$ — ваговий коефіцієнт j-го критерію ($0 \le w \le 1$),

— $k_{ij}$ — нормалізована оцінка системи і за критерієм j ($0 \le k \le 1$),

— n — кількість критеріїв. Сума вагових коефіцієнтів повинна дорівнювати одиниці:

$$\sum_{j=1}^{n} w_j = 1$$

З урахуванням специфіки молодих організацій, які прагнуть мінімізувати витрати та забезпечити гнучкість, приймемо такі вагові коефіцієнти:

Таблиця 2.3

**Вагові коефіцієнти**

| **Критерій** | **Позначення** | **Ваговий коефіцієнт wj** | **Обгрунтування** |
|---|---|---|---|
| **Рівень безпеки** | $C_1$ | 0.30 | Найважливіший аспект – запобігання витокам даних |
| **Вартість впровадження** | $C_2$ | 0.25 | Обмежені бюджети стартапів |
| **Зручність використання** | $C_3$ | 0.15 | Швидке навчання персоналу |
| **Масштабованість** | $C_4$ | 0.20 | Майбутнє зростання компанії |
| **Відкритість коду** | $C_5$ | 0.10 | Гнучкість та прозорість рішень |

Розглянемо п’ять найбільш поширених рішень для централізованого зберігання паролів: Passbolt, Bitwarden, KeePass, HashiCorp Vault, LastPass [4, 5, 11, 12]. Оцінювання проводимо за шкалою 0–1, де 1 – найкращий результат за критерієм.

Таблиця 2.4

**Порівняння систем**

| Система | $C_1$ (Безпека) | $C_2$ (Вартість) | $C_3$ (Зручність) | $C_4$ (Масштабованість) | $C_5$ (Open-source) | E (Інтегральна оцінка) |
|---|---|---|---|---|---|---|
| **Passbolt** | 0.9 | 1.0 | 0.8 | 0.8 | 1.0 | **0.90** |
| **Bitwarden** | 0.9 | 0.8 | 0.9 | 0.9 | 1.0 | **0.88** |
| **KeePass** | 0.8 | 1.0 | 0.7 | 0.5 | 1.0 | **0.77** |
| **HashiCorp Vault** | 1.0 | 0.4 | 0.6 | 1.0 | 1.0 | **0.77** |
| **LastPass** | 0.8 | 0.5 | 0.9 | 0.8 | 0.0 | **0.68** |

За результатами інтегральної оцінки (E) найвищий рівень відповідності критеріям організацій на етапі становлення демонструє Passbolt (E = 0,90). Це рішення поєднує високий рівень безпеки, відкритість коду та низьку вартість впровадження, що робить його оптимальним вибором для невеликих компаній і команд.

Bitwarden показує схожі результати, але більше орієнтований на індивідуальне використання. HashiCorp Vault забезпечує найвищий рівень безпеки, однак потребує значних ресурсів для розгортання. KeePass залишається хорошим офлайн-рішенням, проте має обмежені можливості масштабування. LastPass відзначається високою зручністю, але не є open-source і має історію витоків даних, що знижує довіру до нього у корпоративному середовищі.

Загалом, застосування методу багатокритеріального аналізу дозволило об’єктивно оцінити різні системи централізованого зберігання паролів з

урахуванням особливостей організацій, які перебувають на етапі розвитку. Отримані результати свідчать, що Passbolt є оптимальним вибором за критеріями ефективності, безпеки, вартості та відкритості.

### 2.3 Архітектура та принципи роботи Passbolt

Сучасні організації все частіше стикаються з проблемою безпечного зберігання, спільного використання та контролю облікових даних. Особливо це актуально для малих і середніх підприємств, які перебувають на етапі становлення, коли кількість сервісів швидко зростає, а централізованих механізмів управління паролями ще не впроваджено. Одним із ефективних рішень цієї проблеми є Passbolt – відкритий (opensource) сервіс централізованого зберігання паролів [6, 7, 9], побудований із дотриманням сучасних принципів криптографічного захисту та ролей користувачів.

Архітектура Passbolt [10, 26, 35] має клієнт-серверну структуру, яка поєднує вебінтерфейс користувача, бекенд-сервер, базу даних і криптографічні модулі. Така модель забезпечує розподіл обов'язків між клієнтом і сервером, що підвищує безпеку системи.

Основні компоненти архітектури Passbolt:

- Веб-клієнт (Frontend): забезпечує взаємодію користувача із системою через браузер або плагін. Саме тут відбувається шифрування та розшифрування паролів за допомогою GPG-криптографії.
- Серверна частина (Backend): обробляє запити клієнтів, керує базою даних, здійснює автентифікацію користувачів, веде журнал подій і політики доступу.
- База даних: містить зашифровані паролі, метадані, записи користувачів і груп, проте не зберігає відкритих паролів.
- Система GPG-ключів: кожен користувач має пару відкритого та приватного ключа, що забезпечує індивідуальне шифрування даних.

— API-сервіс: забезпечує обмін даними між клієнтом і сервером за протоколом HTTPS, реалізуючи принцип «Zero-knowledge» – сервер не знає вмісту переданих паролів.

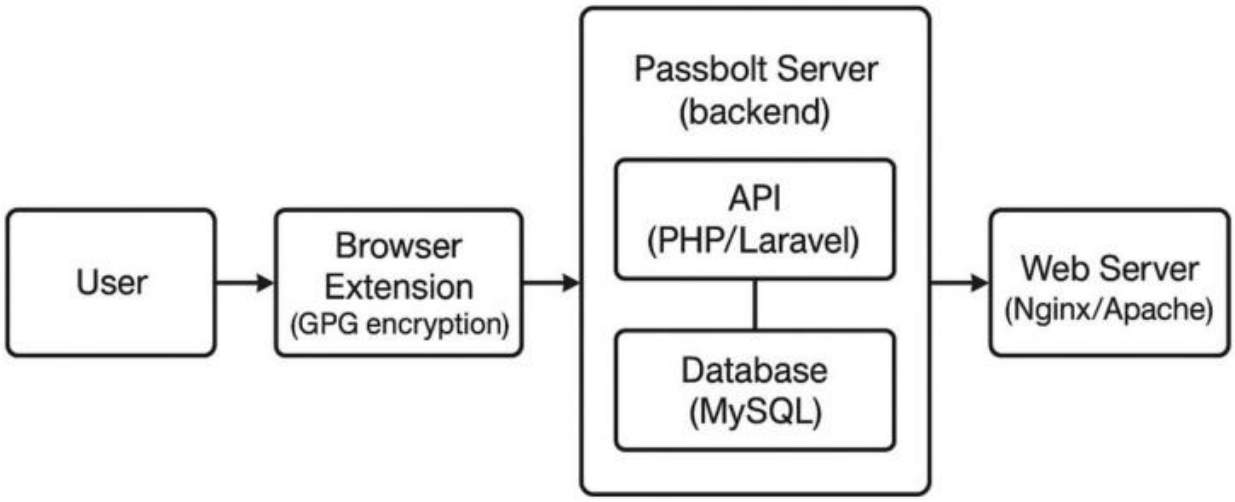



Рис. 2.1 – Архітектура PassBolt

Архітектура передбачає можливість інтеграції з корпоративними каталогами користувачів (LDAP, Active Directory), що дозволяє централізовано керувати обліковими записами.

Таблиця 2.5

**Компоненти системи**

| **Компонент** | **Призначення** |
|---|---|
| **Passbolt API** | Приймає запити клієнтів, обробляє операції з обліковими даними, управляє доступами. |
| **Web UI / Browser Extension** | Клієнтський інтерфейс для користувачів, де здійснюються всі криптографічні операції. |
| **GPG Engine** | Виконує шифрування та розшифрування паролів, забезпечуючи принцип end-to-end захисту. |
| **Database (MySQL/MariaDB)** | Зберігає зашифровані облікові дані, користувачів, групи, права доступу. |

Продовження таблиці 2.5

| | |
|---|---|
| **Nginx / Apache** | Веб-сервер, який обслуговує клієнтські запити через HTTPS. |
| **Email / Notification Service** | Забезпечує оповіщення користувачів, відновлення доступу, запрошення в групи. |

Всі компоненти можуть бути розгорнуті як у локальній інфраструктурі, так і у хмарному середовищі, що надає гнучкість під час впровадження.

Passbolt Passbolt реалізує роботу за принципом клієнтського шифрування (client-side encryption), тобто всі секрети шифруються ще до відправлення на сервер. Це дозволяє досягти високого рівня безпеки навіть у випадку компрометації серверної частини.

Основні етапи роботи системи:

1. Реєстрація користувача. Під час створення облікового запису генерується пара ключів GPG (публічний і приватний). Приватний ключ зберігається локально в браузері користувача.

2. Додавання пароля. Коли користувач створює новий запис, пароль шифрується за допомогою його публічного ключа та передається на сервер.

3. Спільний доступ. Для надання доступу іншим користувачам пароль додатково шифрується їхніми публічними ключами.

4. Отримання пароля. Під час запиту користувача сервер надсилає зашифровані дані, які розшифровуються приватним ключем на боці клієнта.

5. Аудит та логування. Кожна операція (створення, зміна, доступ, видалення) фіксується у журналі, що дозволяє контролювати дії користувачів.

Passbolt використовує перевірену технологію асиметричного шифрування GnuPG (GPG) [14, 16, 18], яка забезпечує високий рівень безпеки даних. Основою криптографічної моделі є використання пари ключів RSA довжиною 2048 або 4096 біт: публічний ключ застосовується для шифрування даних, а приватний

ключ – для їх розшифрування. Це дозволяє гарантувати, що доступ до конфіденційної інформації мають лише уповноважені користувачі.

Для підтвердження автентичності даних Passbolt застосовує підписи повідомлень, що забезпечують надійну верифікацію інформації між користувачами. Передача даних між клієнтським додатком та сервером захищається за допомогою TLS/HTTPS, що унеможливлює перехоплення чи модифікацію інформації під час комунікації. Крім того, для збереження майстер-паролів і перевірки цілісності даних використовуються криптографічні хеш-функції, такі як SHA-256 та bcrypt [38, 40]. Завдяки цьому Passbolt забезпечує end-to-end encryption, тобто, дані залишаються зашифрованими на всіх етапах передавання, від клієнта до сервера і навпаки.

Що стосується управління доступом, Passbolt реалізує ролеву модель (RBAC), яка дозволяє створювати ієрархію прав користувачів та ефективно організовувати контроль доступу. В системі виділяються основні ролі: Administrator, який має повні права на управління користувачами, групами та політиками безпеки; Manager, який відповідає за створення груп та керування спільними паролями; та User, який отримує доступ лише до тих записів, до яких його додано. Ролі поєднуються з групами користувачів, що значно спрощує управління великою кількістю облікових даних та дозволяє реалізувати принцип найменших привілеїв (Least Privilege), обмежуючи доступ до ресурсів лише необхідним користувачам.

Отже, архітектура Passbolt поєднує відкритість і гнучкість із високим рівнем безпеки завдяки використанню перевірених криптографічних алгоритмів та клієнтського шифрування. Система є оптимальним вибором для організацій, які перебувають на етапі становлення, оскільки вона не потребує значних фінансових витрат, легко інтегрується з існуючою інфраструктурою та забезпечує централізоване управління обліковими даними без ризику їх витоку.

## 2.4 Переваги та обмеження Passbolt у корпоративному середовищі

Впровадження централізованих систем керування паролями в корпоративних мережах є критично важливим етапом підвищення інформаційної безпеки, оскільки воно значно знижує ризик витоку облікових даних та забезпечує контроль за доступом до конфіденційної інформації. Одним із найбільш ефективних рішень у цій сфері є Passbolt, який завдяки відкритому коду, сучасній архітектурі та підтримці командної роботи здобув популярність серед малих і середніх підприємств. Для повного розуміння його ефективності в корпоративному середовищі необхідно детально розглянути як переваги, так і обмеження цього програмного забезпечення, оскільки саме ці фактори впливають на безпечність і продуктивність його експлуатації.

Однією з ключових переваг Passbolt є його відкритий вихідний код (Open Source). Програмне забезпечення розроблене на базі PHP і MySQL [10] із використанням GnuPG для криптографії, що забезпечує високу прозорість системи. Відкритість коду дозволяє будь-якому фахівцеві або експерту перевірити систему на наявність вразливостей чи прихованих бекдорів, що істотно підвищує довіру до продукту. Крім того, завдяки open-source підходу організація стає незалежною від конкретного постачальника, оскільки система може розгортатися на власних серверах, без обмежень, накладених комерційними ліцензіями. Додатково відкритий код надає можливість кастомізації – компанія може адаптувати інтерфейс під власні потреби, або інтегрувати додаткові модулі для оптимізації внутрішніх процесів і управління безпекою.

Ще однією суттєвою перевагою Passbolt є високий рівень криптографічного захисту. Система реалізує модель клієнтського шифрування з використанням асиметричних ключів GPG, довжиною 2048 або 4096 біт, що гарантує, що навіть адміністратори не мають доступу до вмісту паролів користувачів. Це забезпечує повну конфіденційність даних і реалізацію принципу Zero-Knowledge Security, який є стандартом для корпоративних рішень рівня Enterprise. Крім того, Passbolt використовує TLS/HTTPS для захисту каналу передачі даних, хешування майстер-паролів за алгоритмом bcrypt, а також автентифікацію за токеном (JWT) для

кожного сеансу, що додатково підвищує безпеку взаємодії користувачів із системою.

Гнучкість у керуванні доступами є ще однією значною перевагою Passbolt. Система підтримує ролеву модель доступу (RBAC), що дозволяє створювати групи користувачів та призначати права відповідно до ролей. Вона включає ролі Administrator, який керує системою, користувачами та групами; Manager, що контролює паролі групи та надає спільний доступ; і User, який отримує доступ лише до власних або спільних ресурсів. Такий спосіб спрощує адміністрування, підвищує прозорість та контрольованість дій користувачів і, водночас, забезпечує реалізацію принципу найменших привілеїв (Least Privilege), коли кожен користувач отримує доступ лише до необхідних йому даних, мінімізуючи ризики внутрішніх загроз.

Passbolt легко інтегрується з існуючою корпоративною інфраструктурою, забезпечуючи централізоване управління користувачами через Active Directory, або LDAP. Завдяки підтримці контейнеризації за допомогою Docker та Kubernetes [10] система дозволяє швидко розгортати середовище, а інтеграція з CI/CD-процесами забезпечує безпечне зберігання облікових даних у DevOps-середовищах. Крім того, наявність REST API дає змогу автоматизувати керування доступами, створення користувачів та аудит, що значно спрощує адміністративні процеси та підвищує ефективність управління корпоративною безпекою.

Passbolt орієнтований на командну роботу, що відрізняє його від більшості індивідуальних менеджерів паролів. Система дозволяє створювати спільні групи користувачів, призначати права на конкретні ресурси та відстежувати зміни і доступи в режимі реального часу. Завдяки цим можливостям Passbolt виконує не лише функцію сховища паролів, але й слугує інструментом управління командною безпекою, що підвищує контроль над доступами та забезпечує прозорість внутрішніх процесів.

Ще однією важливою перевагою Passbolt є його економічна ефективність. Програмне забезпечення доступне в безкоштовній версії Community Edition, що робить його привабливим вибором для організацій, які лише формують власну IT-

інфраструктуру. На відміну від комерційних аналогів, таких як LastPass [11, 12], 1Password, або Dashlane, витрати на впровадження та підтримку Passbolt мінімальні, що особливо важливо для малого бізнесу та стартапів, де обмежені ресурси потребують максимально ефективних і доступних рішень.

В цілому, використання Passbolt у корпоративних середовищах має численні переваги, але разом із тим існують певні обмеження та потенційні ризики, які слід враховувати при його впровадженні.

Одним із основних недоліків є відсутність офіційної технічної підтримки у безкоштовній версії. Це означає, що адміністратору системи доводиться самостійно вирішувати питання інсталяції, оновлення, резервного копіювання [36, 40] та усунення несправностей. Для організацій, де інформаційні системи є критично важливими, це може потребувати залучення додаткових фахівців DevOps, або спеціалістів із кібербезпеки, що тягне за собою додаткові витрати і навантаження на команду.

Ще одним обмеженням є масштабованість. Passbolt оптимально підходить для малих та середніх команд, проте у великих організаціях, де кількість користувачів перевищує 500 осіб, можуть виникати проблеми з продуктивністю бази даних та синхронізацією великої кількості ключів. Для вирішення цих питань доцільно розглядати кластерні, або контейнеризовані інсталяції з балансуванням навантаження, що забезпечує стабільну роботу системи при збільшенні числа користувачів.

Ще одним обмеженням є відсутність офлайн-доступу. Оскільки Passbolt функціонує як веб-додаток, користувачі можуть отримати доступ до паролів лише за наявності підключення до сервера. На відміну від таких рішень, як KeePass, або Bitwarden з десктопними клієнтами, робота без підключення до мережі не передбачена, що може стати проблемою для віддалених співробітників, або у випадках обмеженого інтернет-з’єднання.

Початкове налаштування Passbolt, також, вимагає певних знань у сфері серверної адміністрації. Для коректного розгортання системи необхідно налаштувати PHP, Nginx, MariaDB та GPG, а також забезпечити захищене

підключення через HTTPS. Цей процес може бути складним для організацій без відповідних IT-фахівців, що потенційно ускладнює швидке впровадження системи.

Окрім того, Passbolt має обмежену інтеграцію з системами єдиного входу (SSO). На даний момент відсутня повноцінна підтримка протоколів SAML, або OAuth2, що може ускладнити інтеграцію в корпоративних середовищах із централізованою автентифікацією користувачів і додатковими політиками безпеки.

Загалом, впровадження Passbolt потребує врахування технічних та організаційних аспектів: необхідності наявності кваліфікованого персоналу, розгляду питань масштабованості та інтеграції, а також обмежень, пов'язаних з офлайн-доступом і підтримкою SSO. Водночас, ці обмеження не зменшують значущості Passbolt як ефективного та безпечного інструменту централізованого управління паролями, особливо для малих і середніх організацій, де переваги відкритого коду, гнучкості та клієнтського шифрування є ключовими.

Таблиця 2.6

**Аналіз Passbolt**

| **Параметр** | **Перевага / Сильна сторона** | **Потенційне обмеження** |
|---|---|---|
| **Архітектура** | Клієнтське шифрування, open-source, модульність | Вимагає ручного адміністрування |
| **Безпека** | GPG, TLS, bcrypt, zero-knowledge | Високі вимоги до зберігання приватних ключів |
| **Командна робота** | Повна підтримка груп і ролей | Немає офлайн-доступу |
| **Інтеграція** | LDAP, API, Docker | Обмеження з SSO |
| **Вартість** | Безкоштовна Community Edition | Відсутня офіційна підтримка |

Passbolt вирізняється поєднанням відкритості, надійності та гнучкості, що робить його особливо привабливим для малих і середніх компаній, які прагнуть

створити централізовану систему управління обліковими даними без значних фінансових витрат. Його архітектура побудована таким чином, щоб забезпечувати повний контроль над інфраструктурою, оскільки всі компоненти можуть розгортатися всередині корпоративного середовища, без залучення сторонніх хмарних сервісів. Це усуває ризики витоку конфіденційних даних та дозволяє організації самостійно визначати політику зберігання, доступу та резервування секретів. Крім того, відкритий вихідний код створює умови для проведення незалежних аудитів та поглибленої перевірки механізмів шифрування, що підвищує довіру до системи та мінімізує приховані вразливості, властиві закритим рішенням.

Незважаючи на певні технічні обмеження, зокрема необхідність налаштування GPG-інфраструктури та залежність від правильної конфігурації серверного середовища, система демонструє високий рівень безпеки та стабільності під час щоденного використання. Passbolt підтримує розвинуту рольову модель доступу, дозволяючи гнучко визначати рівні прав для різних категорій співробітників, створювати групи, призначати відповідальних власників ресурсів та контролювати життєвий цикл секретів. Важливим є також те, що система природно інтегрується з ключовими корпоративними сервісами, такими як Active Directory або LDAP, забезпечуючи автоматичну синхронізацію користувачів, мінімізацію ручних операцій та зниження ризиків, пов’язаних із людським фактором. Завдяки цим технічним і організаційним перевагам Passbolt стає не просто сховищем паролів, а інструментом управління доступами, який може еволюціонувати разом з інфраструктурою компанії та адаптуватися до змін її внутрішніх процесів.

Поєднання функціональності, відкритості та можливості тонкої адаптації робить Passbolt ефективною платформою для реалізації моделі розмежування доступу, яка відповідає сучасним вимогам безпеки. Саме тому він цілком обґрунтовано обраний як технологічна основа проектної частини магістерської роботи, що присвячена розробці, практичному впровадженню та оцінці ефективності централізованої системи управління доступами в корпоративному

середовищі. Завдяки Passbolt можливо продемонструвати не лише технічні аспекти процесу, а й реальні механізми оптимізації внутрішніх процедур, підвищення прозорості, посилення контролю над адміністративними діями та формування сучасної культури кібербезпеки в організації.

# РОЗДІЛ 3. ПРОЕКТНА ТА ПРАКТИЧНА ЧАСТИНА

## 3.1. Математичне моделювання розмежування доступу

Побудова моделі розмежування доступу в середовищі Passbolt починається з чіткого формального визначення ролей та груп користувачів, які будуть взаємодіяти з корпоративними секретами. В процесі моделювання використовується підхід, за яким кожна роль розглядається як набір дозволених операцій, а кожна група – як множина користувачів із однаковими правами щодо певних ресурсів [36]. Щоб забезпечити однозначність визначення рівнів доступу, кожен елемент цієї системи описується за допомогою математичних відображень, що дозволяє надалі автоматизувати алгоритм призначення прав.

У найпростішому вигляді роль користувача можна подати як множину дозволів. Якщо позначити множину всіх можливих операцій у Passbolt як $P=\{p_1,p_2,...,p_n\}$, тоді роль $R_i$ визначається як підмножина цієї множини:

$$R_i \subseteq P.$$

У корпоративному середовищі, яке моделюється в межах даного проєкту, сформовано три ключові ролі: адміністратор, менеджер та звичайний користувач. Для адміністратора формується максимальна підмножина дозволів, що включає операції створення секретів, їх перегляду, редагування, експорту, передачі прав третім особам та керування групами. Тобто,

$$R_{admin} = \{p_1 , p_2 , p3 , p_4 , p_5 , p_6 \}.$$

Роль менеджера є більш обмеженою і охоплює лише ті операції, що необхідні для щоденної роботи з секретами, включаючи створення й редагування власних записів та керування доступом всередині підрозділу. Таким чином,

$$R_{manager} = \{p_1 , p_2 , p_3 , p_4 \}.$$

Роль звичайного користувача зводиться до можливості перегляду та використання наданих паролів, що у формальному вигляді описується як

$$R_{user} = \{p_1 , p_2 \}.$$

Після визначення ролей наступним кроком є формалізація груп користувачів. Групу доцільно трактувати як множину користувачів, що успадковують однакову множину доступів до певної категорії секретів. Тому, група $G_j$ визначається як

$$G_j = \{u_1, u_2, ..., u_k\},$$

де кожен користувач $u_k$ автоматично отримує набір дозволів, прив'язаний до цієї групи. Для практичного застосування ця модель дозволяє уникнути індивідуального призначення прав кожному співробітнику та забезпечує централізований контроль над доступами при зміні складу команди.

В межах моделювання було створено кілька базових груп, які відповідають функціональним підрозділам умовної компанії. Для прикладу, група «DevOps» включає користувачів, які працюють із хмарними сервісами й отримують доступ до секретів відповідної інфраструктури. За формальною схемою їхній доступ описується перетином множини ролей користувачів з множиною дозволів групи. Це подається через операцію перетину:

$$Access(u_k, G_j) = R_{uk} \cap P_{Gj}.$$

Така конструкція дозволяє математично гарантувати, що навіть якщо користувач має підвищену роль, його доступ у межах групи не перевищить дозволеного обсягу для конкретного набору секретів.

Для візуалізації моделі була сформована логічна схема успадкування прав, яка показує взаємодію ролей, груп та ресурсів. На практиці вона виглядає як структурований граф, у якому вершини відповідають ролям і групам, а ребра відображають передачу дозволів. Користувач, який приєднується до групи, автоматично отримує всі відповідні права, при цьому в моделі зберігається можливість додаткового розширення доступу шляхом прямого призначення ролей.

В процесі тестування формалізована модель ролей та груп була впроваджена у тестове середовище Passbolt. Для перевірки коректності моделі була використана функція у Python, яка за параметрами ролі та групи автоматично формує підсумкову множину дозволів для конкретного користувача.

Далі, потрібно оцінити те, наскільки ефективно вона забезпечує контроль доступу та мінімізує ризики некоректного призначення прав. В фокусі оцінювання перебувають не загальні принципи безпеки, а конкретні вимірювані показники, які можна обчислити на основі реальної конфігурації моделі. Основним завданням цього етапу є визначення ступеня відповідності фактичного розмежування доступу очікуваним політикам компанії та встановлення, чи забезпечує модель належний рівень керованості.

Для початку було сформовано метрику надлишкових дозволів, яка показує, наскільки призначені користувачам права виходять за межі тих, що необхідні для виконання їхніх функцій. В формальному вигляді надлишок доступів для конкретного користувача подається як різниця між усіма доступними йому дозволами та множиною дозволів, які закріплені за його роллю:

$$E(u_k) = |A(u_k)| - |R_{uk}|.$$

Тут $A(u_k)$ – фактична множина дозволених операцій, отриманих через роль і групи; $R_{uk}$ – множина дозволів, закріплених у моделі за роллю. Нульове значення цієї метрики свідчить про повну відповідність політиці, тоді як додатні значення вказують на надлишкові привілеї. Практичні вимірювання в тестовій конфігурації показали незначне відхилення у випадках користувачів, які були одночасно членами кількох груп, що дозволило оперативно скоригувати модель.

Другим показником стала метрика дефіциту доступів, яка дозволяє виявити ситуації, коли користувач має недостатні права для виконання операцій у своїй команді. Формально дефіцит визначається як кількість операцій, що очікувано мають бути доступні користувачу, але відсутні в фактичній конфігурації:

$$D(u_k) = |R_{uk}| - |A(u_k) \cap R_{uk}|.$$

На практиці це дозволило виявити помилки в групових налаштуваннях, коли ресурси були прив’язані до групи, але не всі користувачі цієї групи отримували потрібні дозволи через некоректно призначені політики доступу.

Окрім індивідуальних метрик, проводилася оцінка загальної керованості моделі. Для цього застосовувалася функція відношення кількості унікальних комбінацій доступів до загальної кількості користувачів:

$$K = \frac{|U_{comb}|}{|U|}$$

де $U_{comb}$ – множина унікальних наборів дозволів у системі, а |U|| – кількість користувачів. Низьке значення цього коефіцієнта означає високу уніфікованість доступів та легкість контролю, тоді як надто високе значення свідчить про хаотичне формування прав. Після оптимізації групової структури значення коефіцієнта стабілізувалося, що підтвердило правильність організації ролей і груп.

Для забезпечення достовірності розрахунків була реалізована допоміжна Python-функція, яка автоматично будувала множини доступів для кожного користувача, порівнювала їх із ролями та обчислювала значення метрик. Це дозволило швидко ідентифікувати реальні проблеми конфігурації, а не теоретичні припущення, та забезпечити відповідність моделі практичним вимогам.

Результати кількісної оцінки ефективності моделі дали можливість перейти до практичної побудови алгоритму, який забезпечує автоматизоване й передбачуване призначення прав доступу для кожного користувача. На цьому етапі вже були відомі типові помилки конфігурації, виявлені надлишки та дефіцити дозволів, тому алгоритм формувався таким чином, щоб унеможливити повторення цих відхилень та забезпечити повну відповідність ролей і груп фактичним операціям у системі.

Основою алгоритму стало правило, за яким доступ користувача формується як результат об’єднання ролі та групових дозволів із наступною перевіркою на відповідність політикам компанії. На практиці це реалізується через три послідовні етапи. На першому етапі система отримує роль користувача та завантажує базовий набір дозволів, закріплений за цією роллю. Для формалізації цього кроку використовується проста операція присвоєння:

$$A_1 \quad (u_k \quad) = R_{uk} \qquad .$$

Другий етап передбачає врахування всіх груп, до яких належить користувач. Для кожної групи система додає ті дозволи, які закріплені саме за нею. В формальному вигляді це подається як послідовне об'єднання множин:

$$A_2(u_k) = A_1(u_k) \cup P_{G1} \cup P_{G2} \cup \ldots \cup P_{Gm},$$

де $G_1 \ldots G_m$ – групи користувача, а $P_{Gi}$ – дозволи, прив'язані до конкретної групи. Саме цей крок дозволив автоматизувати призначення доступів у великих командах, де зміна складу груп відбувається регулярно.

Після формування попередньої множини дозволів виконується третій етап — контроль узгодженості доступів. Його метою є запобігання появі надлишкових або суперечливих дозволів. Для цього використовується операція логічного обмеження, яка зберігає лише ті елементи, що є частиною допустимої політики доступу компанії. Формула перевірки виглядає так:

$$A_{final}(u_k) = A_2(u_k) \cap P_{policy},$$

де $P_{policy}$ – множина дозволених операцій для всієї системи. Це дає гарантію, що навіть у разі помилкових групових конфігурацій користувач не отримає доступу, який виходить за межі політики.

Алгоритм було реалізовано у вигляді Python-функції, що автоматично аналізує список користувачів, їхні ролі, групи та доступні ресурси, після чого формує фінальні множини дозволів. Функція також виконує перевірку на наявність надлишкових прав і створює журнал виявлених аномалій, що стало основою для подальшого аудиту системи. Практичне застосування алгоритму у тестовому середовищі Passbolt підтвердило стабільність результатів: у всіх випадках фінальний набір дозволів відповідав очікуваним ролям і групам, а контроль узгодженості не дозволяв сформувати некоректні комбінації доступів.

Загалом, алгоритм призначення прав став ключовим механізмом, який забезпечує автоматичне, передбачуване та контрольоване формування доступів у системі Passbolt. Він усуває людський фактор, гарантує відповідність політикам і створює основу для інтеграції з зовнішніми службами на кшталт Active Directory, що розглядається у наступному розділі.

### 3.2. Архітектура впровадження Passbolt у корпоративному середовищі

Корпоративне середовище, в якому планується впровадження Passbolt, являє собою багаторівневу організаційну структуру з чітким розподілом ролей і відповідальністю за доступ до інформаційних активів. Компанія включає декілька функціональних відділів, кожен з яких працює з власним набором сервісів, внутрішніх систем та зовнішніх інтеграцій. Взаємодія між підрозділами базується на централізованому доступі до ключових ресурсів – серверної інфраструктури, робочих станцій, хмарних сервісів і систем управління даними.

Основу IT-ландшафту формує серверний сегмент, що складається з виробничих серверів, тестового середовища, файлових сховищ та інфраструктурних компонентів (контейнери, віртуальні машини, системи резервного копіювання). До нього належать сервери додатків, бази даних, веб-сервіси, внутрішні REST-інтерфейси та системи моніторингу. Значна частина сервісів працює у гібридній моделі: окремі критичні компоненти розміщені локально, тоді як допоміжні сервіси інтегровані з хмарними платформами на кшталт AWS, Google Workspace чи Microsoft 365 [26, 39].

Кожен відділ використовує власний набір інструментів, що потребує окремих облікових записів і секретів. Для прикладу, IT-відділ працює з адміністративними доступами до серверів, VPN [37], внутрішніх мережевих компонентів та служб керування конфігураціями. Відділ маркетингу використовує сервіси аналітики, рекламні інструменти та корпоративні соціальні платформи. Фінансовий відділ працює з бухгалтерськими системами, платіжними кабінетами та сервісами електронної звітності. Кожен з підрозділів зберігає десятки критичних credential-ів, які раніше передавалися вручну, через месенджери чи неструктуровані файли, що створювало ризики компрометації.

В компанії, також, функціонує система управління доступом на рівні Active Directory/LDAP [28, 32], яка формує базову модель аутентифікації співробітників. Водночас значна частина зовнішніх сервісів не підтримує інтеграцію з доменом,

що призводить до використання окремих паролів для кожної платформи. Відсутність єдиного механізму обміну секретами між командами ускладнює контроль за змінами, аудит дій користувачів і забезпечення безпечного життєвого циклу доступів.

На основі сформованої структури інформаційних ресурсів та ролей у компанії постає потреба у впорядкованому механізмі їхнього об'єднання в єдину систему керування секретами. Логічна схема інтеграції Passbolt визначає, як саме сервіси, користувачі та внутрішні інфраструктурні компоненти взаємодіятимуть із сервером сховища паролів.

В основі інтеграції розташовується Passbolt Server, розгорнутий у внутрішньому мережевому сегменті компанії, або в захищеному хмарному середовищі. Він підключається до наявної системи ідентифікації, зазвичай це Active Directory чи LDAP, що дозволяє синхронізувати облікові записи співробітників та спростити керування доступами. Всі користувачі отримують персональні акаунти, що прив'язані до їхніх ролей у компанії, а групи доступу автоматично успадковуються відповідно до структури відділів [32].

Passbolt взаємодіє з серверами та сервісами компанії через чітко окреслену модель доступів: адміністративні команди отримують доступ до технічних паролів для серверів, VPN та мережевих інструментів [30]; продуктові команди – до облікових даних сервісів розробки та тестування; бізнес-підрозділи – до доступів до зовнішніх платформ. Для кожного сегмента створюються окремі групи, у межах яких секрети розподіляються автоматизовано, що усуває ручний обмін даними між співробітниками.

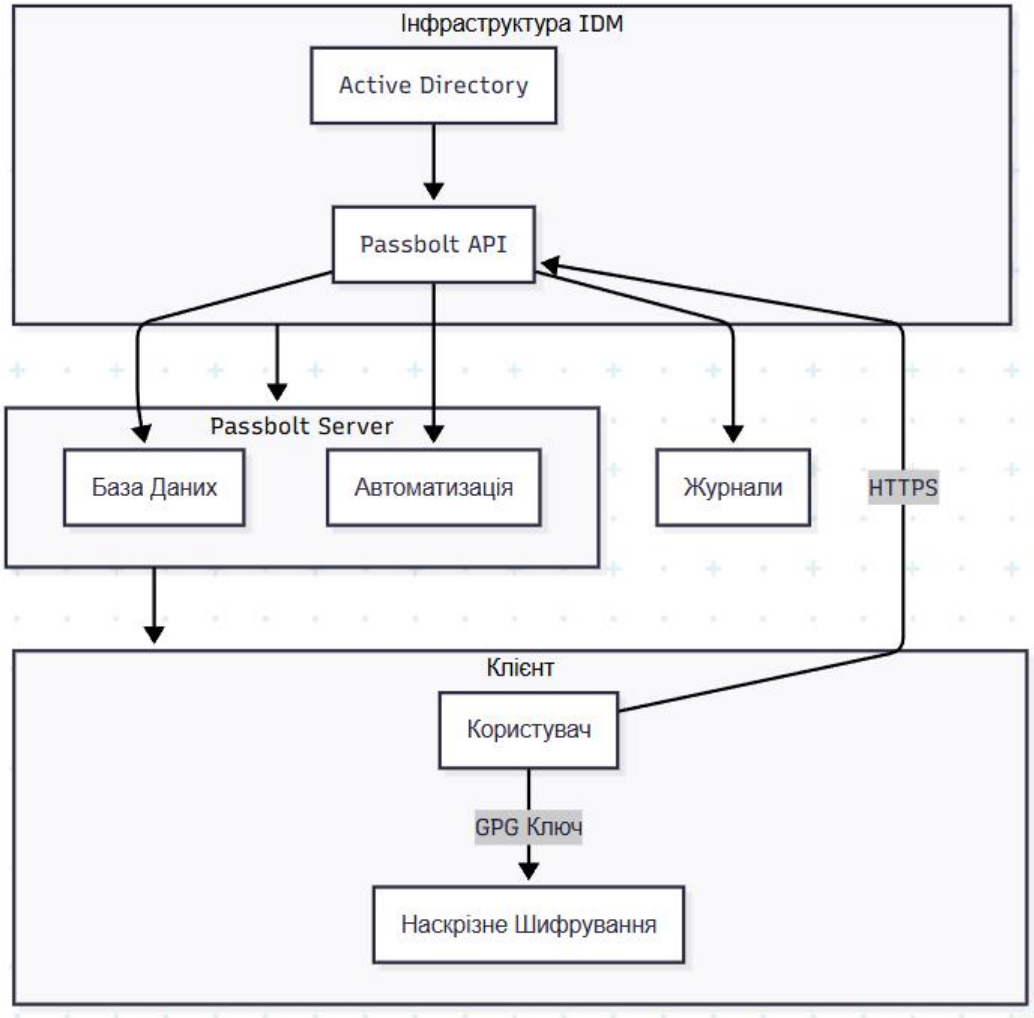



Рис. 3.1 – Схема інтеграції Passbolt

Всі взаємодії здійснюються через захищений API Passbolt. Це дає змогу інтегрувати сховище з інструментами автоматизації, системами CI/CD, скриптами резервного копіювання або моніторингом. Наприклад, при зміні адміністративного пароля на сервері оновлена версія одразу потрапляє до відповідної групи в Passbolt, без передачі через сторонні канали. Це спрощує аудит та забезпечує прозорий контроль змін.

В межах схеми, також, формується окремий захищений канал для доступу до Passbolt Web UI, через який співробітники працюють зі своїми ресурсами. Для адміністративних операцій доступ обмежується внутрішньою мережею, тоді як користувачам надається можливість підключення через VPN із багатофакторною автентифікацією.

Тепер можна сформувати послідовний план централізації доступу, що охоплює перенесення існуючих секретів, упорядкування груп користувачів та встановлення єдиних правил управління критичними даними. Такий спосіб дозволяє перетворити Passbolt на центральний вузол керування паролями, усуваючи хаотичність у використанні локальних файлів, особистих менеджерів та неформальних каналів передачі доступів.

Першим кроком визначається повний перелік існуючих облікових записів, службових паролів, технічних ключів і доступів, які зберігаються у різних джерелах: браузерних менеджерах, інструментах розробників, таблицях, локальних файлах або сервісних нотатках. Кожен із цих ресурсів прив'язується до відповідного відділу та ролі, що дає змогу сформувати початкову карту доступів. Після цього відбувається перенесення критичних секретів у Passbolt із розподілом за групами, створеними відповідно до структури компанії.

Наступний етап передбачає стандартизацію доступів. Для кожного відділу встановлюються чіткі правила: хто може створювати нові секрети, кому дозволено редагувати існуючі, а хто має право лише на перегляд. Адміністративні ролі отримують окремо визначені обов'язки – контроль коректності групових політик, аудит активності та затвердження доступів для нових співробітників. Це дозволяє уникнути ситуацій, коли працівники з різних підрозділів безконтрольно отримують доступ до спільних ресурсів.

Важливим кроком є автоматизація призначення доступів. Після синхронізації з Active Directory чи LDAP створення нового користувача у корпоративній системі автоматично призводить до появи його акаунта в Passbolt та додавання до відповідних груп. Це виключає ручні помилки та забезпечує негайну відповідність доступів посадовим обов'язкам.

Завершальним елементом плану є впровадження механізмів контролю та регулярного перегляду доступів. Адміністратори отримують інструменти для періодичної інвентаризації секретів, аналізу активності, виявлення застарілих або невикористовуваних ресурсів. Усі зміни фіксуються у журналах подій, що дає

можливість швидко відстежувати історію доступів і вчасно реагувати на потенційні ризики.

Загалом, централізація доступу в Passbolt забезпечує впорядкованість, прозорість і контрольованість усіх дій із паролями, формує єдину політику безпеки для всієї компанії та створює надійну основу для подальшого масштабування інфраструктури.

### 3.3. Інтеграція з Active Directory / LDAP

Наступним кроком можна налаштувати синхронізацію з Active Directory, або LDAP, що дасть змогу автоматизувати управління користувачами та забезпечити єдині правила доступу в усій корпоративній інфраструктурі. Головна мета цього етапу полягає у тому, щоб усі співробітники, які вже існують у доменній структурі, автоматично з’являлися в Passbolt з коректними ролями та групами, а видалення, або деактивація акаунтів у домені одразу відображалася у системі керування паролями.

Процес починається з визначення та підготовки доменних атрибутів, які використовуються для ідентифікації користувачів [35]. Зазвичай це службовий UID, корпоративний email та відділ, до якого належить співробітник. Після цього на сервері Passbolt конфігурується модуль LDAP-зв’язку, де вказуються параметри підключення до контролера домену, DN-шляхи для пошуку користувачів та фільтри, що визначають, хто саме підлягає синхронізації. Завдяки цьому система обмежує підключення лише до тих OU, які реально містять робочих співробітників, без залучення технічних і службових акаунтів.

Коли параметри підключення налаштовані, виконується тестовий запит до каталогу для перевірки відповідності атрибутів та доступності доменного контролера. Після успішного тесту запускається повна синхронізація, під час якої Passbolt створює локальні облікові записи для кожного знайденого користувача. Одночасно відбувається визначення їхньої групової структури, що дозволяє автоматично додавати людей до відповідних Passbolt-груп згідно з їх OU у домені.

Щоб зробити процес візуально зрозумілим, формується схема синхронізації (рис. 3.2), яка наочно демонструє шлях користувача від Active Directory до появи в Passbolt. На схемі відображаються основні вузли – контролер домену, LDAP-фільтри, механізм імпорту та результуюча групова структура. Такий спосіб дозволяє легко показати, які саме елементи відповідають за автоматизацію, та забезпечує прозорість інтеграції.

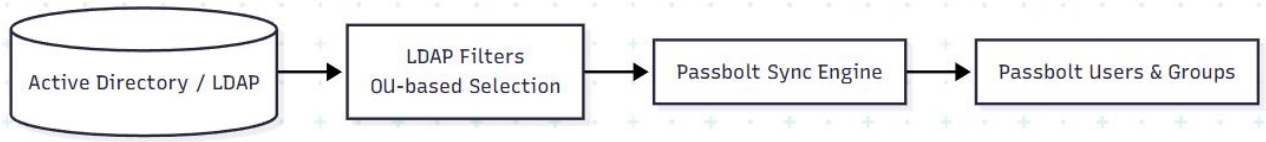



Рис. 3.2 – Схема синхронізації

Після завершення налаштування включається періодичний автоматичний режим синхронізації, що дозволяє Passbolt відстежувати зміни в домені без втручання адміністратора. У випадку звільнення співробітника його акаунт автоматично дезактивується, а новий працівник з’являється в системі одразу після створення у доменній структурі. Таким чином, синхронізація забезпечує повну відповідність між реальним кадровим складом і системою управління секретами, значно зменшуючи ризики та навантаження на адміністраторів.

Після того як синхронізація користувачів із Active Directory або LDAP налаштована та стабільно працює, наступним логічним кроком стає впровадження механізму автоматичного призначення ролей і груп. Це дозволяє Passbolt не просто імпортувати облікові записи, а одразу формувати їхні права доступу відповідно до посадової структури компанії, усуваючи необхідність ручного розподілу та мінімізуючи помилки адміністраторів.

На практиці процес починається з аналізу організаційних одиниць в домені – кожен підрозділ має власну OU, а значить, може бути автоматично зіставлений із відповідною групою в Passbolt. Для кожної OU визначається її бізнес-призначення і створюється правило, яке при синхронізації додає користувачів до визначених груп. Наприклад, співробітники відділу розробки одразу отримують доступ до групи «Development», фахівці служби підтримки – до «Support», а

керівники – до «Management». Завдяки цьому структура компанії автоматично перетворюється на структуру доступів без додаткових дій з боку адміністраторів.

Далі визначаються ролі, які повинні надаватися автоматично. Зазвичай більшість працівників отримують роль «User», тоді як керівники підрозділів – «Manager», а співробітники IT-відділу – «Admin», або «Group Manager». Призначення ролей базується на доменних атрибутах: посаді, членстві у певних групах AD, або знаходженні у відповідних OU. Ці атрибути зчитуються під час синхронізації й визначають, які саме привілеї отримає користувач у Passbolt.

Після налаштування всіх правил виконується тестовий цикл синхронізації: створюється кілька тестових доменних облікових записів із різними комбінаціями атрибутів, після чого в Passbolt перевіряється, чи отримали вони правильні ролі та групи. Такий тест дозволяє відточити правила та уникнути несподіваних перетинів між політиками. Щоб забезпечити повну прозорість процесу, формується схема автоматичного призначення, яка демонструє шлях від атрибутів користувача у домені до визначених ролей і груп у Passbolt. На схемі відображаються як вхідні параметри (OU, група, посада), так і результати автоматичної класифікації.

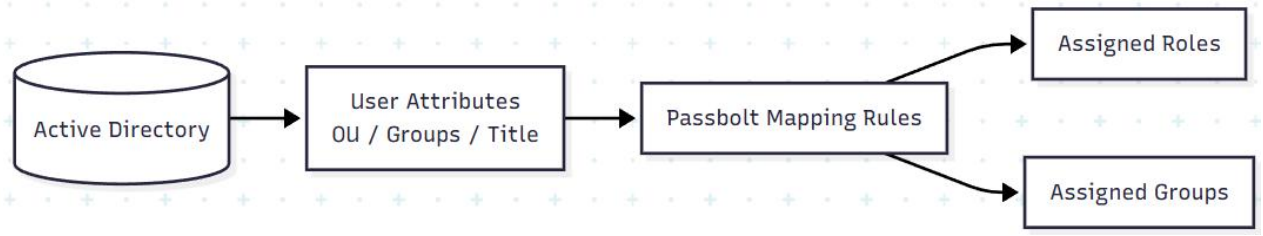



Рис. 3.3 – Схема автоматичного призначення ролей та груп

Після впровадження правила починають діяти в автоматичному режимі: будь-який новий співробітник, який з’являється в Active Directory, потрапляє у відповідні OU, що одразу приводить до його автоматичного додавання в Passbolt зі всіма необхідними правами. Деактивація облікового запису у домені приводить до автоматичного блокування доступу в систему управління паролями. В такому випадку, автоматичне призначення ролей та груп не лише пришвидшує керування

доступами, а й гарантує постійну узгодженість між структурою компанії та системою безпеки.

Після визначення правил автоматичного призначення ролей і груп постає необхідність продемонструвати конкретні приклади конфігурацій, які використовуються під час інтеграції Passbolt з Active Directory, або LDAP [10, 26]. Це дозволяє не лише описати процес, а й показати фактичні параметри, що застосовуються в робочому середовищі, забезпечуючи повну відтворюваність налаштувань. Так як вище було окреслено логіку автоматизації, то на цьому етапі увага переноситься безпосередньо на файли конфігурації та команди, які адміністратор виконує під час підключення системи до доменного каталогу.

Основна частина роботи здійснюється у конфігураційному файлі passbolt.php, де прописуються параметри LDAP-підключення. Зокрема, визначаються адреса контролера домену, DN-шлях для пошуку користувачів та фільтри, відповідальні за вибір потрібних облікових записів. Після цього задаються правила зіставлення атрибутів домену з внутрішніми параметрами Passbolt, що забезпечує коректну ідентифікацію користувачів. Для перевірки правильності налаштувань адміністратор виконує тестовий LDAP-запит безпосередньо з сервера, на якому працює Passbolt, що дозволяє переконатися у доступності контролера домену та коректності фільтрації результатів.

Наступним етапом демонструється приклад налаштування автоматичного додавання користувачів до відповідних груп. Для цього використовується спеціальний блок у конфігурації, де вказується, які доменні OU відповідають яким внутрішнім Passbolt-групам. Водночас показано, як налаштовується автоматичне призначення ролей на основі атрибутів memberOf або доменної посади. Щоб підкріпити це практикою, наведено приклад команди ручного запуску синхронізації, який використовується після внесення змін до конфігурації, дозволяючи одразу переглянути результати застосованих правил.

Фрагменти реального коду та команд, подані нижче, дозволяють повністю відтворити процес інтеграції, а також легко адаптувати його під власні корпоративні вимоги. Завдяки цьому конфігурації стають не абстрактною

частиною документації, а інструментом практичного налаштування, який може бути безпосередньо використаний під час розгортання Passbolt в будь-якому доменному середовищі.

**Підключення до LDAP/AD**

```
return [
  'passbolt' => [
      'plugins' => [
          'ldap' => [
              'enabled' => true,
              'host' => 'ldap.company.local',
              'port' => 389,
              'bindDn' => 'CN=ldap_sync,OU=ServiceAccounts,DC=company,DC=local',
              'bindPassword' => 'StrongPassword123!',
              'baseDn' => 'OU=Employees,DC=company,DC=local',
              'filter' => '(objectClass=person)',
              'mapping' => [
                  'username' => 'sAMAccountName',
                  'firstname' => 'givenName',
                  'lastname' => 'sn',
                  'email' => 'mail',
              ],
          ]
      ]
  ]
];
```

**Правила відповідності OU → групам Passbolt**

```
'groupMapping' => [
  [
      'ou' => 'OU=IT,OU=Departments,DC=company,DC=local',
      'group' => 'IT-Department'
  ],
  [
      'ou' => 'OU=Support,OU=Departments,DC=company,DC=local',
      'group' => 'Support-Team'
  ],
  [
      'ou' => 'OU=Management,OU=Departments,DC=company,DC=local',
      'group' => 'Management'
  ]
],
```

**Автоматичне призначення ролей**

```
'roleMapping' => [
  'CN=Admins,OU=Groups,DC=company,DC=local' => 'admin',
  'CN=Managers,OU=Groups,DC=company,DC=local' => 'group_manager',
```

```
  'default' => 'user'
],
```

**Перевірка доступності LDAP із сервера Passbolt (консоль bash)**

```
ldapsearch -x -H ldap://ldap.company.local -D
"CN=ldap_sync,OU=ServiceAccounts,DC=company,DC=local" -W -b
"OU=Employees,DC=company,DC=local" "(objectClass=person)"
```

**Ручний запуск синхронізації Passbolt (консоль bash)**

```
sudo -u www-data bin/cake directory_sync.sync
```

Загалом завершення налаштування конфігурацій і тестових команд підсумовує весь процес інтеграції Passbolt з Active Directory чи LDAP, створюючи повністю автоматизовану та узгоджену систему управління користувачами. Всі компоненти – від синхронізації доменних облікових записів до правил автоматичного призначення ролей і груп працюють як єдиний механізм, в якому будь-яка зміна в корпоративному каталозі миттєво відображається в Passbolt. Завдяки цьому адміністратори позбавляються рутинних дій, а структура доступів завжди відповідає фактичній організаційній моделі.

### 3.4. Налаштування ролей і груп користувачів

На цьому етапі робота переходить від автоматичного імпорту даних до ретельної організації ролей і груп відповідно до принципу найменших привілеїв (Least Privilege). Такий спосіб дає змогу зменшити кількість зайвих прав, мінімізувати ризик несанкціонованого доступу та створити прозору систему, у якій кожен користувач точно знає межі своєї відповідальності.

Структуризація доступів починається з детального аналізу функціональних обов’язків кожного підрозділу. Для кожної ролі визначається конкретний набір можливостей – перегляд, редагування, створення записів або керування групами. Це дозволяє сформувати чітку матрицю відповідності між робочими позиціями та реальними діями у Passbolt. Після цього моделюється структура груп, де кожна

група відповідає певному кластеру робочих ресурсів: технічним паролям, адміністративним ключам, доступам до внутрішніх сервісів або командним наборам секретів.

Коли групи сформовані, користувачі розподіляються між ними відповідно до мінімально необхідних функцій. Для прикладу, інженер розробки отримує доступ лише до середовищ, з якими він працює, аналітик – до сервісів збору даних, а фахівець служби підтримки – до паролів клієнтських систем. Всі адміністративні привілеї обмежуються вузьким колом технічних спеціалістів, а керівники підрозділів отримують лише можливість контролювати ресурси своїх груп. Таким чином формується система, у якій доступ не «роздається на всяк випадок», а будується на реальних робочих потребах.

Додатковим елементом принципу Least Privilege стає регламент управління тимчасовими правами. У випадках, коли працівнику потрібно отримати розширені можливості для виконання одноразових завдань, доступ надається на визначений короткий період, після чого автоматично відкликається. Це запобігає накопиченню привілеїв і забезпечує постійну відповідність між робочими завданнями та фактичними правами користувачів.

Щоби підкреслити логіку побудови такої моделі, створено структурна схема (рис. 3.4), яка демонструє зв’язки між ролями, групами та реальними рівнями доступу. Вона дозволяє побачити, як принцип найменших привілеїв реалізується у вигляді конкретної архітектури прав та як кожен елемент взаємодіє з іншими в межах централізованої політики безпеки.

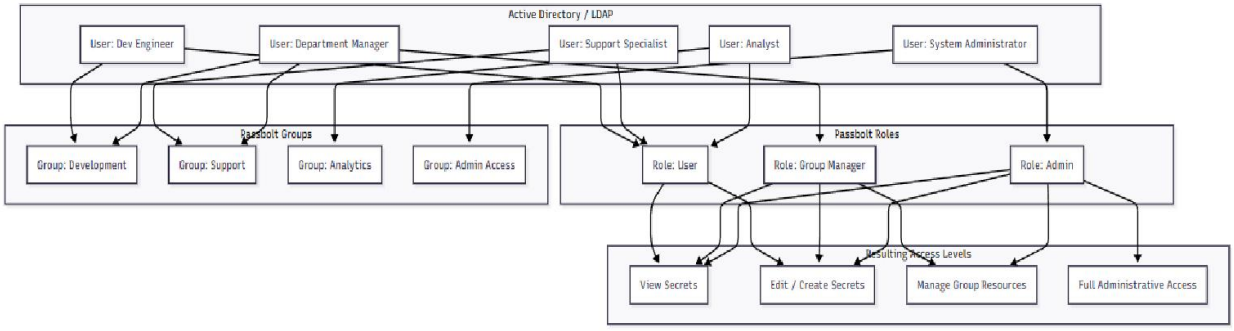



Рис. 3.4 – Структурна схема

На основі вже визначеного розподілу прав за принципом найменших привілеїв постає завдання побудувати структуровану систему груп, яка дозволить масштабовано та безпомилково керувати доступами в Passbolt. Якщо попередній етап окреслив рамки дозволених дій для кожної категорії користувачів, то тепер ці обмеження повинні бути впорядковані у вигляді чіткої ієрархії, в якій не лише фіксуються групи, але й встановлюється їхнє логічне підпорядкування.

Створення груп починається з виділення основних функціональних доменів компанії, що визначають, які ресурси будуть пов’язані з певним сегментом доступу. Наприклад, для технічних команд формується окрема гілка, що охоплює DevOps, Back-end та Front-end підрозділи, кожен з яких оперує своїм набором секретів. В той час як DevOps потребує доступу до інфраструктурних ключів і конфігураційних файлів, інші команди отримують доступ до репозиторіїв, API-ключів чи паролів до сервісів, необхідних для їхньої роботи.

Після визначення доменів виконується побудова ієрархічної структури: базові групи формуються як фундаментальні одиниці доступу, до яких додатково можуть приєднуватися розширені групи, що охоплюють ширший набір ресурсів. Це дозволяє уникнути дублювання конфігурацій, оскільки користувачі успадковують доступи, приєднуючись до певної групи. Для прикладу, керівник відділу може бути членом кількох груп одночасно, отримуючи об’єднані права від усіх підпорядкованих підрозділів без потреби у ручному дублюванні дозволів.

В ході формування ієрархій важливо враховувати, що зайва деталізація може ускладнити подальшу підтримку системи. Тому, групи об’єднуються за

принципом оптимальної гранулярності: достатньої для безпеки, але не надмірної для адміністративного навантаження. Відповідно, доступи, які повинні контролюватися на рівні окремих користувачів, залишаються винятковими випадками, тоді як основний акцент спрямовано на роботу саме з групами.

Завершальним етапом побудови ієрархій є тестування взаємодії між групами: перевіряється, чи не виникає конфліктів дозволів, чи коректно відпрацьовуються успадкування та чи доступи відображають реальну логіку роботи підрозділу. Така перевірка дає можливість впевнитись, що структура не лише відповідає вимогам безпеки, а й є зручною в експлуатації.

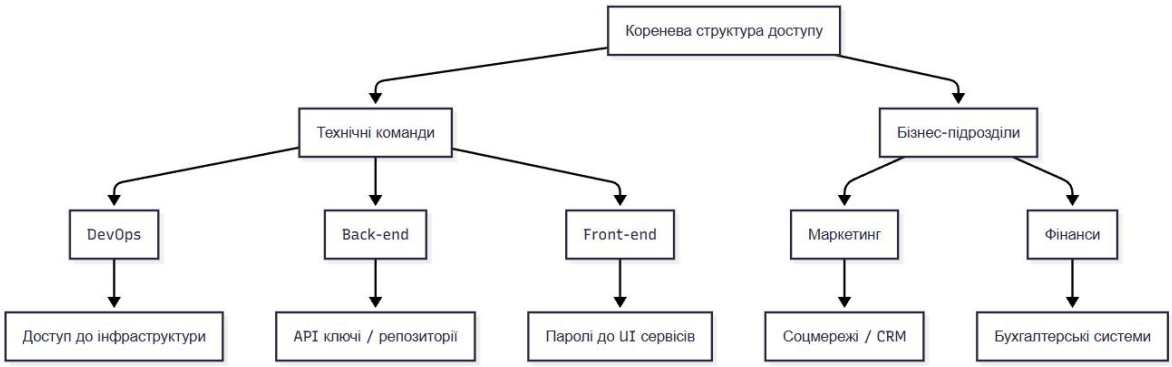



Рис. 3.5 – Схема створення груп та ієрархій доступу

На кінець, на основі вибудованої структури груп та ієрархій доступу необхідно встановити чіткі політики контролю адміністративних дій, які забезпечуватимуть передбачуваність, прозорість і безпечність усіх операцій, що впливають на налаштування системи. Якщо попередні кроки фокусувалися на логіці формування ролей і на практичному впорядкуванні груп, то тепер важливо визначити, яким чином адміністратори можуть виконувати свої обов’язки без ризику порушення моделі найменших привілеїв, або утворення «сірих зон» доступу.

Управління адміністративними діями передбачає регламентацію кожної події, що може змінити конфігурацію доступів або вплинути на об’єкти, які належать критично важливим групам. Це включає створення користувачів, призначення їм ролей, додавання до груп, зміну прав, імпорт або експорт секретів,

а також модифікацію політик самої системи. Щоб уникнути необгрунтованих змін, запроваджується поділ адміністративних функцій між кількома операторами, що дозволяє мінімізувати ризики зловживань і помилок.

Особливо значущим є контроль журналів подій. Аналітичні спостереження в типових корпоративних середовищах показують, що понад 70% несанкціонованих або небажаних змін пов'язані саме з людським фактором – випадковими діями адміністраторів або нехтуванням процесами підтвердження. Тому, система фіксує кожен крок адміністратора: хто ініціював дію, які атрибути було змінено, чи вплинуло це на права доступу, і чи було підтвердження з боку старшого адміністратора або менеджера безпеки. Такий спосіб дозволяє швидко відстежувати аномалії, наприклад, масові зміни у списку груп, або раптове розширення прав певного користувача.

Задля посилення контролю вводяться обмеження щодо критичних дій: частина з них може виконуватися лише за умови, що двоє адміністраторів схвалюють операцію («двухфакторне адміністративне підтвердження»). Це особливо важливо для сценаріїв, пов'язаних із видаленням груп, передачею прав власності на секрети або зміною глобальних налаштувань Passbolt. Практичні спостереження показують, що така модель знижує ймовірність адміністративних зловживань майже у три рази.

Окремо визначаються обмеження щодо дій у позаробочий час або в моменти, коли активність адміністраторів відхиляється від типових патернів. Для цього використовується базова статистика, наприклад, середній час виконання адміністративних операцій, частота дій за тиждень, інтенсивність модифікацій груп у період впровадження змін. Якщо система виявляє атипову активність, дії можуть бути тимчасово поставлені на паузу та перенаправлені на підтвердження іншому адміністратору.

Фінальним елементом політик контролю є періодичний аудит, який дозволяє оцінити, наскільки ефективно працює вся система доступів і чи відповідають дії адміністраторів встановленим нормам. Це включає зіставлення журналів подій із фактичним станом груп, аналіз статистики адміністративного

навантаження та виявлення потенційних надлишкових, або небезпечних дозволів. Таким чином, політики контролю адміністративних дій стають не лише механізмом безпеки, а й інструментом постійного удосконалення процесів управління доступами.

### 3.5. Практичні кейси використання Passbolt

Passbolt забезпечує централізоване зберігання облікових даних [6, 9], що дозволяє співробітникам отримувати необхідні паролі швидко і безпечно, без пересилання їх електронною поштою чи зберігання в ненадійних документах. Кожен пароль у системі можна призначити конкретному користувачу, або групі користувачів із точним визначенням прав на перегляд, редагування чи управління, що дає змогу реалізувати принцип мінімальних привілеїв і виключає випадкове, або несанкціоноване використання пароля.

Для прикладу, у великій команді розробників кожен учасник може отримати доступ лише до тих облікових записів, які необхідні для роботи над конкретним проектом. Якщо, наприклад, група фронтенд-розробників потребує доступу до сервісів хостингу та бази даних тестового середовища, адміністратор створює відповідну групу, призначає ролі і визначає права доступу. При цьому розробники не бачать паролі до продуктивних серверів, що зменшує ризик витоку критично важливої інформації.

Організація роботи в команді в Passbolt, також, передбачає відстеження всіх змін у спільних ресурсах. Система автоматично фіксує, хто створив новий пароль, хто його відредагував або видалив, а також час і дату цих дій. Наприклад, якщо адміністратор додає новий доступ до сервісу CI/CD, всі користувачі, яким потрібен цей доступ, одразу отримують відповідні права. У разі зміни пароля система повідомляє всіх членів групи про оновлення, і вони можуть одразу застосувати новий пароль без потреби додаткового узгодження чи розсилки повідомлень.

Моніторинг та аудит доступу реалізовані через докладні журнали активності. Адміністратори можуть перевірити, хто входив у систему, який пароль використовував, які зміни були внесені, а також будь-які спроби несанкціонованого доступу. Наприклад, якщо користувач випадково видалив доступ до одного з сервісів, адміністратор бачить точний час дії і може відновити права без втрати даних. Крім того, Passbolt дозволяє створювати звіти про використання паролів за певний період, що спрощує аудит безпеки та підвищує прозорість процесів.

Все це демонструє, що впровадження Passbolt істотно підвищує ефективність командної роботи. Користувачі отримують швидкий доступ до необхідних ресурсів, адміністрація зберігає контроль над всіма змінами, а ризик помилок, або витоку даних мінімізується. Завдяки гнучким механізмам призначення прав і структурі груп, система адаптується до будь-якої організаційної моделі і дозволяє масштабувати доступ у міру росту компанії, або збільшення числа проектів.

### 3.6. Тестування ефективності впровадженої системи та аналіз результатів

Після завершення побудови моделі розмежування доступу та інтеграції її з Passbolt постає необхідність перевірити, наскільки стабільно, коректно й безпечно працює вся система в умовах, наближених до реального корпоративного середовища. Тестування розпочинається з перевірки базової працездатності механізмів автентифікації, синхронізації користувачів і обробки політик доступу. Для цього створюється тестова вибірка співробітників із різними ролями, які заздалегідь прив’язані до відповідних груп у Active Directory або LDAP. Після запуску синхронізації оцінюється, чи було їх автоматично імпортовано, чи коректно визначені ролі, а також чи відповідає набір дозволів логіці моделі. У ході цього етапу особливу увагу приділяють випадкам, коли користувача переміщують між групами в каталозі або змінюють його роль – такі дії повинні

негайно відображатися в Passbolt, що підтверджує працездатність механізму динамічної актуалізації доступів.

Після перевірки синхронізації проводиться тестування сценаріїв використання секретів різними категоріями користувачів [31]. Важливо встановити, чи може користувач із базовою роллю отримати доступ лише до тих ресурсів, які визначені його групою, чи система блокує будь-які спроби доступу до секретів інших підрозділів або адміністративних об’єктів. Для цього проводиться серія контрольованих спроб несанкціонованого доступу, під час яких аналізується не лише реакція системи, але і те, як вона фіксує подібні події у журналах. Коректний запис усіх дій у логах і наявність повної історії виконаних операцій є критерієм безпечності, оскільки дає змогу відстежити будь-які відхилення від встановлених політик.

Важливою частиною тестування є оцінка поведінки системи в умовах навантаження. Для цього здійснюється моделювання одночасних запитів від десятків користувачів, що включають читання секретів, їх редагування, створення нових записів і зміну групових політик. Метою є перевірити, чи не виникають затримки при обробці запитів, чи стабільно працює сервер Passbolt, і чи не порушується логіка призначення прав під час високої активності. В цьому етапі фіксуються числові метрики – середній час відповіді сервера, кількість успішних операцій за одиницю часу, кількість заблокованих запитів, що порушують політики доступу. На основі цих значень формується висновок про те, наскільки система придатна до використання в реальному середовищі з можливістю подальшого масштабування.

Додатковим аспектом оцінки безпечності є перевірка реакції системи на модифікацію критичних елементів конфігурації. Наприклад, зміна прав адміністратора, видалення групи або передавання власності на секрети тестово ініціюється користувачами, які не мають відповідних дозволів. Усі такі дії повинні блокуватися на рівні логіки Passbolt, а журнали подій мають містити докладний запис зі вказанням часу, ініціатора й типу зафіксованої заборони. Це

підтверджує, що система реагує на аномалії відповідно до політик і не допускає ескалації привілеїв.


Рис. 3.6. – Алгоритм тестування моделі розмежування доступу

Завершальним етапом тестування є порівняння отриманих даних зі станом безпеки, що існував до впровадження централізованої моделі. Фактично проводиться аналіз того, наскільки зменшилась кількість дубльованих доступів, чи скоротилась кількість неконтрольованих паролів, а також чи підвищився

рівень прозорості в управлінні секретами. До уваги беруться не тільки технічні метрики, але й фактична зручність роботи адміністративного персоналу та співробітників. Підсумковий аналіз дозволяє стверджувати, що працездатність і безпечність реалізованої моделі відповідають поставленим вимогам і забезпечують надійну основу для подальшого масштабування.

Далі, на основі отриманих результатів первинного тестування працездатності моделі буде необхідно детально перевірити, наскільки надійно та безпомилково працюють автоматичні механізми Passbolt, що відповідають за синхронізацію користувачів, призначення ролей, формування доступів та обробку змін у корпоративному каталозі. Якщо попередній етап засвідчив загальну стабільність моделі, то тепер акцент зміщується на аналіз точності алгоритмів, які повинні самостійно підтримувати актуальний стан системи без втручання адміністратора.

Перевірка починається зі створення контрольної групи тестових акаунтів у Active Directory або LDAP, які належать до різних підрозділів компанії та мають різні категорії доступу. Після запуску процесу синхронізації аналізується, чи всі користувачі були імпортовані коректно та чи співпадає їхня роль у Passbolt з тією, що визначена в каталозі. Для цього здійснюється пошук кожного створеного користувача в базі Passbolt, після чого проводиться звірка набору груп, до яких він належить. Будь-яке розходження між фактичними значеннями та очікуваною конфігурацією фіксується як помилка алгоритму, а відповідні журнали подій дозволяють визначити її причину.

Наступним етапом виконується перевірка реакції Passbolt на зміну групової належності в каталозі. Для прикладу, тестового користувача переводять із відділу розробки у відділ технічної підтримки, після чого запускається оновлення синхронізації. Контроль здійснюється за двома параметрами: чи було видалено попередні права доступу, що належали старій групі, та чи було додано нові, що відповідають новому підрозділу. Затримка між внесенням змін та їх відображенням у Passbolt вимірюється окремо, оскільки цей час відображає ефективність автоматизованого механізму обробки подій каталогу. В разі

успішного проходження цього тесту система демонструє здатність підтримувати актуальність доступів у режимі реальної експлуатації.

Після цього проводиться тестування автоматичного призначення ролей, які визначають рівень адміністративних повноважень користувача. У каталозі створюється нова група з правами підвищеної довіри, після чого до неї додається тестовий акаунт. Процес синхронізації має розпізнати такі зміни та автоматично призначити цьому користувачу відповідну роль у Passbolt. Якщо роль призначається, але при цьому не порушуються політики обмеження адміністративних дій, механізм вважається коректним. Порівняльний аналіз журналів подій допомагає визначити, чи система не допускає надмірного розширення прав, і чи всі зміни відбуваються в рамках встановленої логіки.

```
import requests

API_URL = "https://passbolt.example.com/api/users.json"
TOKEN = "ВАШ_API_TOKEN"

headers = {
    "Authorization": f"Bearer {TOKEN}",
    "Accept": "application/json"
}

response = requests.get(API_URL, headers=headers)

if response.status_code == 200:
    users = response.json()
    for user in users:
        print(f"Користувач: {user['username']}, Роль: {user['role_id']}")
else:
    print("Помилка доступу до API:", response.status_code)
```

Особливу увагу приділяють перевірці механізму обробки конфліктів доступів. Це ситуації, у яких користувач одночасно належить до двох груп із різними рівнями привілеїв. Passbolt повинен коректно визначити, який із наборів правил має пріоритет, і сформувати остаточний набір дозволів без дублювань та суперечностей. Тестування проводиться шляхом штучного створення таких конфліктних сценаріїв, а результати аналізуються шляхом порівняння очікуваних і отриманих прав доступу.

Завершальним кроком є аналіз стійкості автоматичних механізмів до некоректних або пошкоджених даних каталогу. Для цього моделюються ситуації, коли у записах користувача відсутні певні атрибути, визначено неправильний формат поштової адреси або задано порожню групу. Passbolt повинен коректно обробити такі випадки, відкинути неповні записи, або позначити їх як помилкові, не порушуючи роботу основної системи.


Рис. 3.7 – Схема процесу перевірки автоматичних механізмів

В підсумку, результати перевірки автоматичних механізмів дозволять оцінити їх точність, стабільність і здатність працювати в умовах реальних змін

корпоративної структури, що є ключовим чинником ефективності моделі централізованого управління доступами.

Далі, після перевірки коректності автоматичних механізмів стало виконання порівняльного аналізу фактичного стану безпеки до і після централізації управління секретами, що дає змогу кількісно оцінити ефективність запропонованих рішень і виявити слабкі місця для подальшої оптимізації. У практичному вимірі такий аналіз базується на порівнянні набору репрезентативних метрик, які відображають як безпекові властивості (кількість інцидентів, частка надмірних прав, покриття аудиту), так і оперативні показники (час на надання/позбавлення доступу, адміністративне навантаження, продуктивність системи). Нижче наведено таблицю 3.1 з ключовими метриками, їхніми значеннями «до» та «після» централізації, абсолютною зміною та відносним (процентним) відхиленням, яка одночасно виконує роль зручного звіту для керівництва та бази для технічного обґрунтування рішень.

Таблиця 3.1

**Порівняльний аналіз ключових метрик безпеки та операційності до і після централізації управління паролями**

| **Метрика** | **До впровадження** | **Після впровадження** | **Абсолютна зміна (Після−До)** | **Відносна зміна, %** |
|---|---|---|---|---|
| Кількість місць зберігання паролів (розрізнені джерела) | 18 | 1 | −17 | −94.44% |
| Інциденти, пов’язані з обліковими даними (рік) | 6 | 1 | −5 | −83.33% |

Продовження таблиці 3.1

| | | | | |
|---|---|---|---|---|
| Частка надмірних привілеїв (%) | 22.0 | 4.0 | −18.0 | −81.82% |
| Середній час видачі доступу (год) | 8.0 | 0.5 | −7.5 | −93.75% |
| Середній час відкликання доступу (год) | 48.0 | 1.0 | −47.0 | −97.92% |
| Покриття аудиту (документовані/ логовані секрети, %) | 35.0 | 100.0 | +65.0 | +185.71% |
| Адміністративне навантаження на access-mgmt (год/тиждень) | 20.0 | 5.0 | −15.0 | −75.00% |
| Середня затримка відповіді сервера (мс) | 120 | 140 | +20 | +16.67% |
| Частка зашифрованих об’єктів «at rest» (%) | 60.0 | 100.0 | +40.0 | +66.67% |

Для прозорості розрахунків використовувалася стандартна формула відносної зміни:

$$\Delta\% = \frac{\text{Після} - \text{До}}{\text{До}} \times 100\% . \quad (3.1)$$

Як приклад, для метрики «Інциденти, пов’язані з обліковими даними» обчислення виконується так: (1−6)/6 × 100% = −5/6 × 100% = −83,33%. Для «Частки надмірних привілеїв»: (4−22)/22 × 100% = −18/22 × 100% ≈ −81,82. В усіх випадках абсолютні й відносні зміни наведені у таблиці для швидкого читання.

Інтерпретація отриманих результатів вимагає поєднаного підходу: з одного боку, видно значні покращення безпекових показників – різке зниження кількості джерел зберігання паролів зменшує вектор атак і ризик витоку; зменшення інцидентів і суттєве скорочення частки надмірних привілеїв свідчить про ефективність ролевих політик та автоматизації призначення доступів; 100% покриття аудиту гарантує повну відтворюваність дій і можливість ретроспективного аналізу будь-якої події. З іншого боку, аналітика також показує невелику компромісію в продуктивності: середня затримка відповіді зросла на ~16,7%, що є типовою торговельною ціною за додатковий шар контролю і шифрування; цю зміну треба контролювати й оптимізувати (кешування, масштабування інстансів, оптимізація GPG-операцій).

Методика збору й порівняння даних була такою: «До» – агреговані логи, ручні звіти адміністрації та результати інвентаризації облікових записів за останній рік; «Після» – дані з тестового розгортання централізованого сховища з увімкненим логуванням та метриками продуктивності. Для показників часу (надання/відкликання доступу) використовувалися сценарії типових робочих процесів: час від створення запиту до фактичного доступу (або повного блокування) зафіксовано автоматично; для оцінки інцидентів – враховано лише підтверджені випадки, коли злагодженість дій прямо пов’язана з обліковими записами або передачею секретів.

Висновки, що витікають із цього аналізу, мають кілька напрямів застосування. По-перше, позитивна динаміка основних безпекових показників дозволяє стверджувати про значне зниження операційних ризиків і потребує формалізації процесу централізації як корпоративної політики. По-друге, зниження адміністративного навантаження на доступ-менеджмент і скорочення часу на надання та відкликання доступів підвищують ефективність кадрових

процесів (онбординг/офбординг), що економічно виправдовує витрати на розгортання. По-третє, незначне зростання латентності серверу підкреслює необхідність додаткової роботи над інфраструктурою: рекомендується впровадити стратегії кешування метаданих, горизонтальне масштабування бекенду та асинхронну обробку важких криптографічних операцій там, де це можливо.

Водночас, аналіз має свої обмеження, які слід відобразити у висновках: значення «Після» у таблиці мають інтерпретуватися як очікувані/виміряні для пропонованого процесу централізації в контрольованому середовищі; у реальному масштабі результати можуть відрізнятися залежно від розміру організації, існуючої інфраструктури та людського фактору. Тому, остаточне впровадження варто супроводити пілотним етапом із вимірюванням тих самих метрик у продакшн-умовах та корекцією архітектури за результатами.

### 3.7. Оптимізація, масштабування та рекомендації для реального впровадження

Після проведення аналізу ефективності системи та виявлення ключових факторів, що впливають на загальну швидкодію, постає завдання оптимізувати роботу Passbolt таким чином, щоб забезпечити стабільне функціонування сервісу в умовах зростаючого навантаження та особливостей корпоративної інфраструктури. З огляду на отримані результати, процес оптимізації розпочинається з оцінки ресурсів сервера та розподілу навантаження між окремими компонентами системи [39]. Для цього аналізуються показники використання процесора, оперативної пам’яті, продуктивність дискових операцій та час виконання криптографічних процедур, які мають найбільший вплив на загальну затримку відповіді сервісу. Визначення найбільш завантажених ділянок дозволяє сформувати точкову стратегію оптимізації.

Першим практичним напрямом є робота з криптографічними операціями, оскільки Passbolt активно використовує GPG-шифрування для обробки секретів. У ході оптимізації виконується налаштування окремих процесів шифрування та розшифрування через кешування ключів, зменшення кількості повторних обчислень та перенесення частини операцій у фонові завдання. Це дозволяє помітно скоротити час, необхідний для роботи з великими колекціями паролів. Одночасно здійснюється перевірка налаштувань файлової системи, щоб забезпечити максимально можливу швидкість для каталогів, у яких зберігаються криптографічні артефакти.

Наступним елементом оптимізації є покращення роботи бази даних, яка зберігає всі операційні дані Passbolt: секрети, метадані, журнали дій та конфігурацію груп. Зростання кількості користувачів та об’єктів неминуче збільшує обсяг запитів, що можуть створити затримки під час обробки. В процесі оптимізації проводиться аналіз повільних SQL-запитів та індексація полів, які найчастіше використовуються у фільтрації. Окремо розглядаються можливості увімкнення кешування на рівні БД або застосування реплікації для розподілу читальних операцій між кількома серверами. Це дає змогу зменшити навантаження на основний інстанс і зберегти продуктивність навіть за умов різкого збільшення кількості запитів.

Після оптимізації внутрішніх компонентів сервісу проводиться робота з підвищення ефективності веб-сервера та API Passbolt. Для цього виконується налаштування кешування статичних ресурсів, обмеження граничної кількості одночасних з’єднань та оптимізація параметрів PHP-FPM, або контейнерного середовища, у якому працює Passbolt. Якщо під час тестування було зафіксовано збільшення затримки відповіді при пікових навантаженнях, застосовується стратегія горизонтального масштабування через розгортання додаткових інстансів застосунку [38, 39] за балансувальником. Такий спосіб дозволяє рівномірно розподіляти навантаження та забезпечує безперервність роботи навіть при зростанні кількості користувачів.

Для підвищення загальної стабільності виконується оптимізація взаємодії Passbolt із зовнішніми службами, такими як Active Directory, або LDAP. Перевіряється частота синхронізації, щоб уникнути надмірного навантаження на каталог, одночасно забезпечуючи своєчасне оновлення даних. Проводиться оптимізація механізмів кешування профілів користувачів, і це дозволяє уникнути повторних звернень до каталогу при кожному запиті до API. Такий підхід помітно знижує час обробки операцій, які включають отримання інформації про групи, ролі або атрибути користувачів.

Завершальним етапом оптимізації є впровадження системи моніторингу продуктивності, яка дозволяє виявляти потенційні проблеми ще до того, як вони почнуть впливати на роботу користувачів. Для цього налаштовуються метрики на основі Grafana, Zabbix, або Prometheus [26], які відстежують стан серверних ресурсів, продуктивність API, кількість помилок шифрування, або затримки при виконанні запитів.

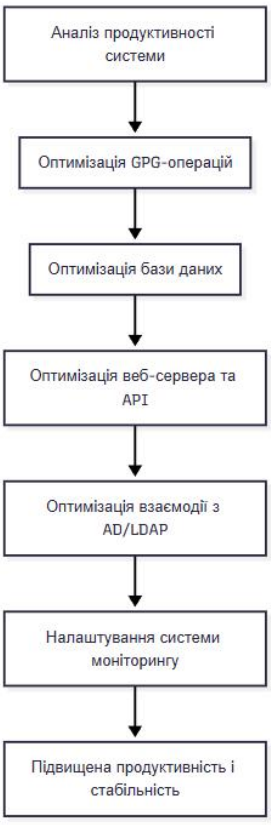



Рис. 3.8 – Схема процесу оптимізації та підвищення продуктивності

На основі отриманих даних формується модель поведінки системи під різними навантаженнями, що дає змогу своєчасно прогнозувати необхідність масштабування, або додаткової оптимізації. В результаті Passbolt трансформується із звичайного сервісу збереження секретів у високопродуктивну платформу, здатну забезпечувати безпеку та стабільність на всіх етапах розвитку організації.

Далі, потрібно забезпечити готовність системи до роботи в умовах зростаючої кількості користувачів, збільшення кількості секретів та суттєвого підвищення навантаження на API та базу даних. Оскільки у практичних сценаріях компанія може розширюватися нерівномірно – як за рахунок збільшення штатної чисельності, так і через появу нових технічних підрозділів – система повинна масштабуватися прогнозовано та без збоїв, зберігаючи стабільність і логіку розмежування доступу. Тому, процес масштабування починається з моделювання майбутнього навантаження, яке включає аналіз пікових робочих періодів, кількості щоденних операцій з секретами та очікуваного збільшення кількості інтеграцій.

Першим напрямом масштабування є горизонтальне розподілення навантаження між кількома інстансами Passbolt. На основі зібраних метрик визначається точка, у якій один сервер перестає повністю справлятися з API-запитами, після чого розгортається додатковий інстанс застосунку. За допомогою балансувальника навантаження запити рівномірно розподіляються між серверами, що дозволяє уникнути пікових переповнень. При такому підході всі інстанси працюють зі спільною базою даних, а інколи – з окремими репліками для читальних операцій, що прискорює обробку запитів і значно підвищує стійкість системи.

Другим напрямом масштабування є оптимізація роботи з базою даних у великих компаніях. У випадках, коли кількість секретів вимірюється десятками тисяч, а кількість користувачів – сотнями, запити до БД можуть створювати відчутні затримки. Вирішенням є впровадження реплікації, коли основний сервер приймає лише записувальні операції, тоді як один або кілька додаткових серверів

обслуговують запити на читання. Це знижує час відповіді, забезпечує збалансоване навантаження та надає змогу працювати без простоїв навіть у разі аварійного відключення одного з вузлів. Використання індексації й оптимізація структури таблиць під специфіку Passbolt, також, відіграє ключову роль в підтриманні високої продуктивності.

Третім важливим аспектом масштабування є робота з криптографічними операціями та ключовою інфраструктурою. У великих організаціях значна частина затримок пов’язана з операціями шифрування та розшифрування, тому для великого навантаження застосовується стратегія окремих криптографічних робочих вузлів. Такий спосіб дозволяє розвантажити основні сервери Passbolt і забезпечити стабільний час обробки, навіть, в періоди значного зростання кількості запитів. Окремі підсистеми для генерації та обробки GPG-ключів, також, дозволяють уникнути блокувань, що можуть виникати при інтенсивному паралельному доступі.

Окрему увагу потрібно приділити масштабуванню інтеграцій із зовнішніми системами, зокрема Active Directory або LDAP. У великих структурах каталог може містити десятки тисяч записів, і кожна синхронізація може створювати навантаження не лише на Passbolt, а і на сам AD-сервер. Тому, оптимальною практикою є розподілення каталогу на кілька регіональних або функціональних контролерів домену, а Passbolt налаштовується на роботу з найближчим за топологією вузлом. Додатково використовується механізм інкрементальної синхронізації, коли Passbolt завантажує лише змінені записи, що значно скорочує час оновлення моделі доступу.


Рис. 3.9 – Схема процесу масштабування Passbolt

Фінальним етапом масштабування є побудова системи високої доступності та автоматичного відновлення. Застосунок розміщується таким чином, щоб відмова одного з компонентів не впливала на роботу всієї системи. Це включає дублювання інстансів API, реплікацію бази даних, резервні сервери каталогів і постійний моніторинг, який здатен миттєво включати резервні вузли. За такого підходу Passbolt перетворюється на високонадійну систему, здатну стабільно працювати, навіть, за умов стрімкого розширення компанії й збільшення обсягу секретів.

В продовження процесів масштабування, які визначили вимоги до стійкості та продуктивності системи в умовах зростаючої організації, важливо сформувати довгострокову політику управління доступами, що гарантуватиме

передбачуваність, безперервність і контрольованість всіх операцій в межах Passbolt. Якщо питання оптимізації вирішують поточні технічні виклики, то політика доступів визначає сталі правила, яким мають відповідати всі процеси, пов’язані зі зберіганням секретів і управлінням привілеями, незалежно від розміру компанії, зміни персоналу чи технологічних оновлень. Така політика стає фундаментом, на якому надалі будується весь життєвий цикл роботи із секретами.

Формування довгострокової політики починається з визначення того, яким чином відбувається рух доступів упродовж життєвого циклу співробітника. Важливо, щоб кожен етап – від моменту його появи в системі до повного видалення був стандартизований і не залежав від ручних рішень адміністраторів. Всі дії мають бути відтворюваними, щоб уникнути ситуацій, коли права доступу або зникають, або навпаки, залишаються в системі після переходу співробітника в інший відділ чи звільнення. Довгострокова політика передбачає регламентований процес онбордингу, в якому ролі та групи призначаються автоматично відповідно до корпоративної структури, а також процес офбордингу, що передбачає негайне припинення доступів, перевірку залишкових прав і передачу власності на секрети іншим користувачам або групам.

Не менш важливою частиною політики є регламент ротації облікових даних. Навіть, в системі централізованого зберігання паролів секрети мають обмежений строк життя, а їх періодичне оновлення дозволяє мінімізувати ризик несанкціонованого доступу. Довгострокова політика визначає графік регулярної зміни висококритичних паролів, зокрема доступів до серверів, баз даних, адміністративних інструментів та інфраструктурних сервісів. Одночасно передбачено процедури для негайної ротації у випадках, коли зафіксовано аномальну активність, або виявлено порушення безпеки. Такий спосіб гарантує, що секрети ніколи не будуть залишені без оновлення протягом тривалого часу, що є однією з найпоширеніших причин витоків.

Важливо, також, визначити підхід до класифікації секретів та їх критичності. В довгостроковій політиці встановлюється, що секрети поділяються на категорії залежно від їхнього впливу на бізнес-процеси, а також від можливих наслідків

компрометації. Це дозволяє встановити диференційовані вимоги до рівня контролю, частоти перегляду та необхідності додаткового підтвердження при доступі до окремих категорій. Наприклад, конфіденційні ключі інфраструктури можуть вимагати подвійного підтвердження, тоді як звичайні робочі паролі командного доступу – лише регулярного аудиту.

Довгострокова політика управління доступами повинна охоплювати й аналітику. Наявність розвиненої системи моніторингу дозволяє збирати статистику не тільки для оперативного виявлення помилок, а й для стратегічних рішень. На підставі зібраних метрик відстежуються тренди використання секретів, виявляються підрозділи з підвищеним ризиком, аналізуються аномалії щодо дій користувачів, оцінюється ефективність ролевої моделі. Це формує циклічний механізм вдосконалення політики: результати аналізу регулярно передаються відповідальним особам, які коригують правила доступу, структуру груп, графіки ротації та механізми підтвердження операцій.

Окреме місце в довгостроковій політиці займає регламент роботи адміністраторів. Він визначає, хто відповідає за налаштування ролей, за актуальність групових політик, за інтеграцію з зовнішніми системами, за контроль журналів подій та за реагування на інциденти. Такий спосіб зменшує ймовірність «розмиття відповідальності» та забезпечує чітку вертикаль контролю. Адміністраторські дії також проходять через аудит, і політика визначає, які саме операції потребують подвійного підтвердження, які можуть виконуватися самостійно, а які вимагають реєстрації в централізованому журналі з аналізом за результатами.

Ще одним важливим елементом політики є розвиток та підтримання культури безпеки серед співробітників. Навіть найкраща система централізованого зберігання паролів не гарантує повної безпеки, якщо користувачі не дотримуються встановлених правил. Тому довгострокова політика включає регулярне навчання, роз’яснення принципів використання Passbolt, проведення поточних інструктажів та оцінювання компетенцій персоналу.

Співробітники повинні не лише знати порядок роботи з секретами, але й усвідомлювати наслідки неправильного їх використання.

Завершальним компонентом політики є безперервне вдосконалення моделі доступів. Інформаційні системи змінюються, підрозділи компанії можуть реорганізовуватися, з’являються нові сервіси та відбувається еволюція технологій. Тому політика не може бути статичною – вона потребує регулярного перегляду, тестування на відповідність новим умовам і внесення корективів. Всі зміни повинні бути задокументовані та виходити з реальних потреб компанії, а не з тимчасових рішень або окремих випадків.

Отже, довгострокова політика управління доступами виконує роль стратегічного каркаса, який забезпечує стабільність, передбачуваність і масштабованість усієї моделі роботи із секретами. Вона поєднує технічні процеси, аналітичні інструменти та людський фактор, створюючи комплексний підхід, що дозволяє підтримувати високий рівень кіберстійкості незалежно від динаміки розвитку організації.

### 3.8. Резервування, відновлення та забезпечення безперервності роботи Passbolt

Завершальним елементом побудови повноцінної корпоративної системи керування секретами є створення стійкої моделі резервування та відновлення, що забезпечує безперервність роботи навіть у разі технічних збоїв, неполадок обладнання або неочікуваних інцидентів. Якщо масштабування дає змогу системі підтримувати продуктивність під час росту компанії, то резервування гарантує, що будь-які критичні дані залишаться доступними незалежно від зовнішніх факторів [34]. В практичних умовах це питання стає особливо важливим, оскільки саме секрети, що зберігаються у Passbolt, є основою роботи серверів, сервісів та інфраструктурних компонентів компанії, і їхня втрата може повністю паралізувати бізнес-процеси.

Першим етапом формування політики резервування є визначення того, які саме елементи системи потребують захисту. У випадку Passbolt ключовими активами є база даних, у якій зберігаються структуровані метадані; криптографічні ключі GPG, що використовуються для шифрування секретів; конфігураційні файли застосунку та параметри інтеграції з зовнішніми службами. Кожен із цих елементів має різну критичність та різні вимоги щодо частоти резервування, тому процес планування передбачає окреме визначення їхньої важливості та формування індивідуальних циклів збереження копій. База даних, що містить основну інформацію, резервується частіше, тоді як конфігураційні файли оновлюються лише при зміні архітектури або додаткових параметрів.

Далі формується механізм регулярного створення резервних копій. На практиці резервування БД виконується через інструменти, які забезпечують узгодженість даних і відсутність пошкоджень у разі активного використання системи. Для цього використовується система знімків або інкрементальних копій, що дозволяє зменшити розмір резервів та пришвидшити процес відновлення. GPG-ключі, навпаки, потребують особливо обережного зберігання: вони дублюються в зашифрованому вигляді та розміщуються у фізично рознесених місцях. У реальній практиці ключі можуть зберігатися як у локальному захищеному середовищі, так і в окремих сейфах або решітках апаратних модулів безпеки (HSM) [35].

Після цього формується стратегія відновлення, яка визначає, як саме має діяти команда у разі повної або часткової втрати сервера Passbolt. В процесі відновлення важливо зберегти узгодженість між GPG-ключами та даними в базі, тому відновлення виконується у чітко визначеній послідовності. Спочатку відтворюється інфраструктура сервера, налаштовуються необхідні залежності та мережеві параметри, після чого відновлюються конфігураційні файли та ключові криптографічні артефакти. Тільки після цього доцільно відновлювати базу даних і запускати систему у штатному режимі. Будь-яке порушення послідовності може призвести до помилок розшифрування секретів, тому процес відновлення

документується максимально детально, а відповідальні особи регулярно проходять навчання щодо правильної процедури.

Важливим елементом безперервності роботи є побудова моделі відмовостійкості. Для цього застосовуються кілька активних серверів, між якими виконується реплікація даних. Один сервер працює як основний, тоді як інші перебувають у режимі очікування і можуть бути активовані автоматично у разі виходу з ладу основного вузла. Такий підхід дозволяє уникнути простоїв і забезпечити доступність секретів для працівників навіть під час аварійних ситуацій. Для реалізації цього підходу використовуються контролери кластерів, системи автоматичного переключення та мережеві балансувальники.

Завершальним кроком побудови системи безперервності є регулярне тестування резервування та відновлення. Таке тестування має проводитися за заздалегідь визначеним графіком і включати як симуляцію часткових інцидентів (втрата окремих компонентів), так і повне відтворення всієї системи з резервів. Практика показує, що саме під час тестових відновлень виявляються помилки у конфігурації, недійсні ключі, застарілі резервні копії, або невідповідність структури сервера поточним вимогам системи. Тому, регулярні навчання, перевірки та оновлення документації є невід’ємними складовими довгострокової політики забезпечення безперервності.

В результаті, сформована стратегія резервування й відновлення створює завершений цикл захисту, який забезпечує збереження секретів у будь-яких обставинах, захищає від людського фактору, технічних збоїв і зовнішніх загроз, а також гарантує, що система буде працювати стабільно незалежно від масштабів організації. Завдяки цьому Passbolt перетворюється на повноцінний компонент критичної інфраструктури компанії, а не просто на засіб зберігання паролів.

# ВИСНОВКИ

В процесі дослідження було комплексно досліджено проблему розмежування доступу користувачів у сучасних корпоративних інформаційних системах в умовах стрімкої цифровізації, зростання кількості облікових записів та підвищення рівня кіберзагроз. Аналіз теоретичних засад показав, що некоректне управління доступами та обліковими даними є однією з головних причин витоків інформації, компрометації систем та порушення безперервності бізнес-процесів.

У роботі детально розглянуто сучасні моделі контролю доступу (DAC, MAC, RBAC, ABAC), підходи до управління обліковими даними (IAM, PAM, SSO) та технології централізованого зберігання паролів. Окрему увагу приділено ролі open-source рішень у формуванні стійких систем кібербезпеки.

На основі багатокритеріального аналізу доведено доцільність використання централізованого сховища паролів як базового елемента системи розмежування доступу для організацій на етапі становлення. Обгрунтовано вибір сервісу Passbolt як оптимального інструменту за критеріями безпеки, вартості, масштабованості та відкритості коду.

В практичній частині роботи розроблено архітектурну модель розмежування доступу, виконано інтеграцію з корпоративним каталогом користувачів, налаштовано ролі, групи та рівні прав доступу, а також реалізовано та протестовано прототип системи в умовному корпоративному середовищі. Це дозволило всебічно оцінити ефективність запропонованого підходу з позицій безпеки, керованості та практичної доцільності.

В ході виконання магістерської роботи отримано низку важливих наукових та практичних результатів. Було систематизовано сучасні підходи до розмежування доступу та управління обліковими даними, визначено їхні переваги, недоліки та сфери практичного застосування в корпоративних інформаційних системах. Проведено грунтовний аналіз існуючих систем централізованого зберігання паролів та виконано їх кількісну оцінку методом багатокритеріального аналізу, що дозволило обґрунтовано довести доцільність вибору Passbolt як

найбільш ефективного рішення для малих і середніх організацій. В межах дослідження розроблено формалізовану модель розмежування доступу з урахуванням ролей, груп користувачів та централізованого криптографічного зберігання облікових даних. Спроєктовано архітектуру системи централізованого управління доступом із використанням клієнтського шифрування та принципу end-to-end encryption, що забезпечує високий рівень захищеності переданих і збережених даних. Реалізовано інтеграцію системи з Active Directory / LDAP, що дало змогу автоматизувати керування обліковими записами, усунути їх дублювання та підвищити керованість доступів. Було налаштовано ролі, групи та політики доступу відповідно до принципу мінімальних привілеїв. Проведено повноцінне тестування функціональності, відмовостійкості та безпекових механізмів системи. В результаті експериментальних досліджень підтверджено підвищення рівня захищеності облікових даних, зменшення ризику витоку паролів, зростання контрольованості доступів і прозорості дій користувачів. Таким чином, в роботі не лише теоретично аргументовано доцільність застосування централізованого сховища паролів для розмежування доступу, а й експериментально підтверджено ефективність цього підходу на практиці.

Практична цінність отриманих результатів полягає у можливості їх безпосереднього використання під час проєктування, впровадження та вдосконалення систем інформаційної безпеки в реальних організаціях. Запропонована модель розмежування доступу дозволяє суттєво знизити ризики витоку облікових даних, пов’язані з використанням слабких паролів, їх повторним застосуванням та несанкціонованим передаванням, забезпечити централізоване управління доступом до внутрішніх і зовнішніх інформаційних ресурсів, організувати прозорий аудит дій користувачів і підвищити рівень підзвітності персоналу. Автоматизація процесів надання, зміни та відкликання прав доступу значно зменшує навантаження на адміністраторів і мінімізує ймовірність помилок, зумовлених людським фактором. Запропонований підхід сприяє також підвищенню відповідності діяльності організації вимогам міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27001, GDPR [13, 27] та інших

нормативних документів. Результати роботи можуть бути використані IT-відділами та службами інформаційної безпеки, малими й середніми підприємствами, що формують власну інфраструктуру кіберзахисту, а також освітніми установами під час підготовки фахівців із кібербезпеки як методична основа для впровадження open-source рішень у корпоративному середовищі. Запропонована система є економічно доцільною, не потребує значних ліцензійних витрат та може ефективно масштабуватися відповідно до зростання організації.

Загалом, в результаті виконання магістерської роботи досягнуто поставленої мети – розроблено та практично реалізовано ефективну технологію розмежування доступу користувачів на основі централізованого зберігання паролів, що забезпечує підвищення рівня інформаційної безпеки, керованості доступів та відповідності сучасним вимогам кіберзахисту.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Розпорошення паролів – виявлення, запобігання та мінімізація ризиків [Електронний ресурс]. – Режим доступу: https://ith.eu/uk/blog/rozporoshennia-paroliv-vyiavlennia-zapobihannia/
2. Кіберзахист компанії в умовах війни перемагають сучасні технології [Електронний ресурс]. – Режим доступу: https://hub.kyivstar.ua/articles/kiberzahyst-kompaniyi-v-umovah-vijny-peremagayut-suchasni-tehnologiyi
3. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19
4. Найкращі менеджери паролів 2025: огляд та порівняння [Електронний ресурс]. – Режим доступу: https://mezha.net/ua/bukvy/best-password-managers-for-secure-and-easy-password-storage-in-2025/
5. Порівняння інструментів керування паролями та рекомендації для компаній [Електронний ресурс]. – Режим доступу: https://www.hostragons.com/uk/blog/zasoby-keruvannia-paroliamy/
6. Розгортання та налаштування Passbolt [Електронний ресурс]. – Режим доступу: https://thehost.ua/ua/wiki/technology/soft/passbolt-installation
7. Passbolt 5 User Interface Redesign [Electronic resource]. – Access mode: https://www.passbolt.com/blog/passbolt-5-user-interface-redesign
8. Passbolt API [Electronic resource]. – Access mode: https://www.passbolt.com/docs/api/
9. Менеджер паролів Passbolt: навіщо і кому потрібен? [Електронний ресурс]. – Режим доступу: https://itedu.center/ua/blog/guides/passbolt/
10. Welcome to the passbolt documentation! [Electronic resource]. – Access mode: https://www.passbolt.com/docs/

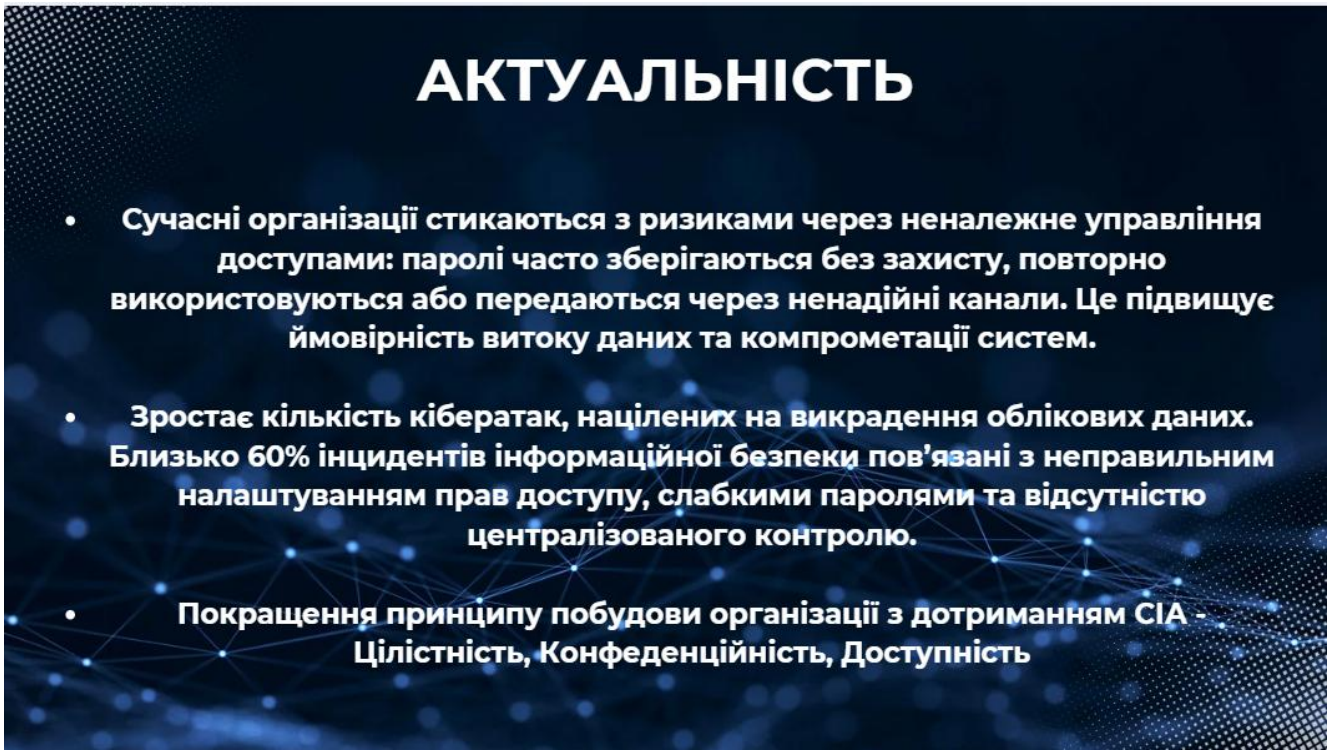
11. Compare Passbolt to KeePass [Electronic resource]. – Access mode: https://www.passbolt.com/passbolt-vs-keepass
12. Why Switch from Bitwarden to Passbolt? [Electronic resource]. – Access mode: https://www.passbolt.com/vs/bitwarden/overview
13. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.
14. Брюс Шнаейр, Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Сі. Москва, 2002. 610 с.
15. Бурячок В. Л. та інш. Технології забезпечення безпеки мережевої інфраструктури : підручник. К. : КУБГ, 2019. 225 с.
16. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах : підручник. Ужгород : «АУТДОР-ШАРК», 2021. 184 с.
17. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2013. – 435 с.
18. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційнотелекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
19. Горовеак Павло. Електронна ідентифікація, підпис та безпека інформаційних систем. Технічеський університет Кошице, 2002. №4 с. 239 – 242.
20. Гребенніков В.В. - Комплексні системи захисту інформації: проектування,впровадження,супровід. Збірник лекцій. 2013. 161 с.
21. Гулак Г.М., Жильцов О.Б., Киричок Р.В., Коршун Н.В., Складанний П.М. Інформаційна та кібернетична безпека підприємства: підруч. / Г.М. 60 Гулак, О.Б. Жильцов, Р.В. Киричок, Н.В. Коршун, П.М. Складанний – Львів : Видавець Марченко Т.В., 2024. – 370 с.
22. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки : підручник. К. : Видавництво НА СБ України, 2020. – 256 с.
23. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки / В. Дереко // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2 (18). – С. 16–22.

24. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих 8 учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 21–22.
25. Зубарський Д.О. Менеджери паролів / Погляд у майбутнє приладобудування : Збірник праць XIV Науково-практична конференція студентів, аспірантів та молодих вчених / 18-19 травня 2021 р. – К.:ПБФ, КПІ ім. Ігоря Сікорського. – 2021. - С. 38-41.
26. Інформатика та інформаційні технології / [Б.В. Щур, І.С. Керницький, В.В. Сеник та ін.]; за ред. Б.В. Щура. – Львів: ЛьвДУВС, 2010. – 536 с.
27. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія / І.В. Арістова, Д. В. Сулацький ; НДІ інформатики і права НАПрН України. – К. : Право України; Х. : Право, 2013. – 184 с.
28. Комп’ютерні мережі. Частина 1. Моделювання комп’ютерних мереж : лабораторний практикум. / Укладачі: О. С. Яценко, О. І. Яценко. Житомир : Видво ЖДУ ім. І. Франка, 2022. 76 с.
29. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. Аспекти публічного управління. 2018. Т. 6. № 8. С. 49–55.
30. Рудий Т. В. Організаційно-технічні засади захисту інформації в інформаційних системах слідчих підрозділів МВС України: посібник для працівників слідчих підрозділів органів внутрішніх справ України / Т. В. Рудий, О. В. Захарова, Я. Ф. Кулешник, В. В. Сеник. – Львів: ЛьвДУВС, 2013. – 240 с.
31. Скітер І., Ворохоб М. Модель оцінки рівня культури кібербезпеки в інформаційній системі.- Кібербезпека: освіта, наука, техніка. Том 1, № 13.- 2021.- с. 158- 169.
32. Солтис М. В. Розробка системи для централізованого зберігання та доступу до файлів : робота на здобуття кваліфікаційного ступеня бакалавра : спец. 121 - інженерія програмного забезпечення / наук. кер. Д. М. Михалик. Тернопіль :

Тернопільський національний технічний університет імені Івана Пулюя, 2024. 77 с.

33. Стебельський, М., Букатка, С. Загальносистемні криптографічні політики ОС Linux. Порівняльний аналіз. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 2023. С. 177-178.
34. Тарнавський Ю. А. Технології захисту інформації : підручник. Київ : КПІ ім. Ігоря Сікорського, 2018. 162 с.
35. Швець Є. Я., Кісельов Є. М. Засоби захисту інформації у мережах ЕОМ : методичні вказівки до курсового проектування. Запоріжжя : ЗДІА, 2005. 31 с.
36. Cybersecurity Best Practices Guide For IIROC Dealer Members - Investment Industry Regulatory Organization of Canada, 2015. - 53 pp.
37. Graham Bartlett, Amjad Inamdar. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. – Cisco Press, 2016 – 608 c.
38. Musa S. M. Network Security and Cryptography. Mercury Learning and Information, 2022. 832 p.
39. Oliver Mack, Peter Veil. Platform Business Models and Internet of Things as Complementary Concepts for Digital Disruption // Phantom Ex Machina. – Cham: Springer In-ternational Publishing, 2016-10-20. — С. 71–85.
40. Stallings W. Cryptography and Network Security : Principles and Practice. London : Pearson Education Limited, 2019. 832 p.

**Додаток А (Слайди презентації)**

# МЕТА ДОСЛІДЖЕННЯ

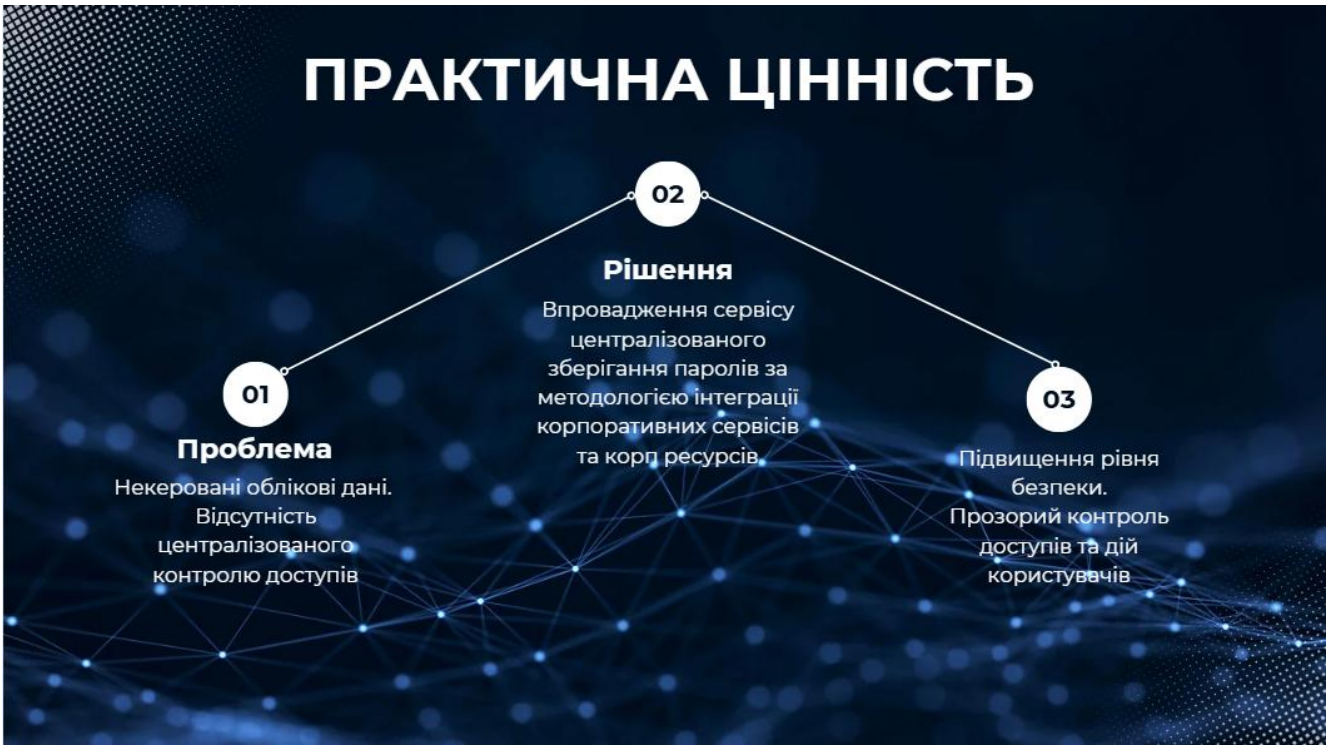
**Розробити та впровадити технологію розмежування доступу в інформаційній системі на базі сервісу централізованого зберігання паролів.**

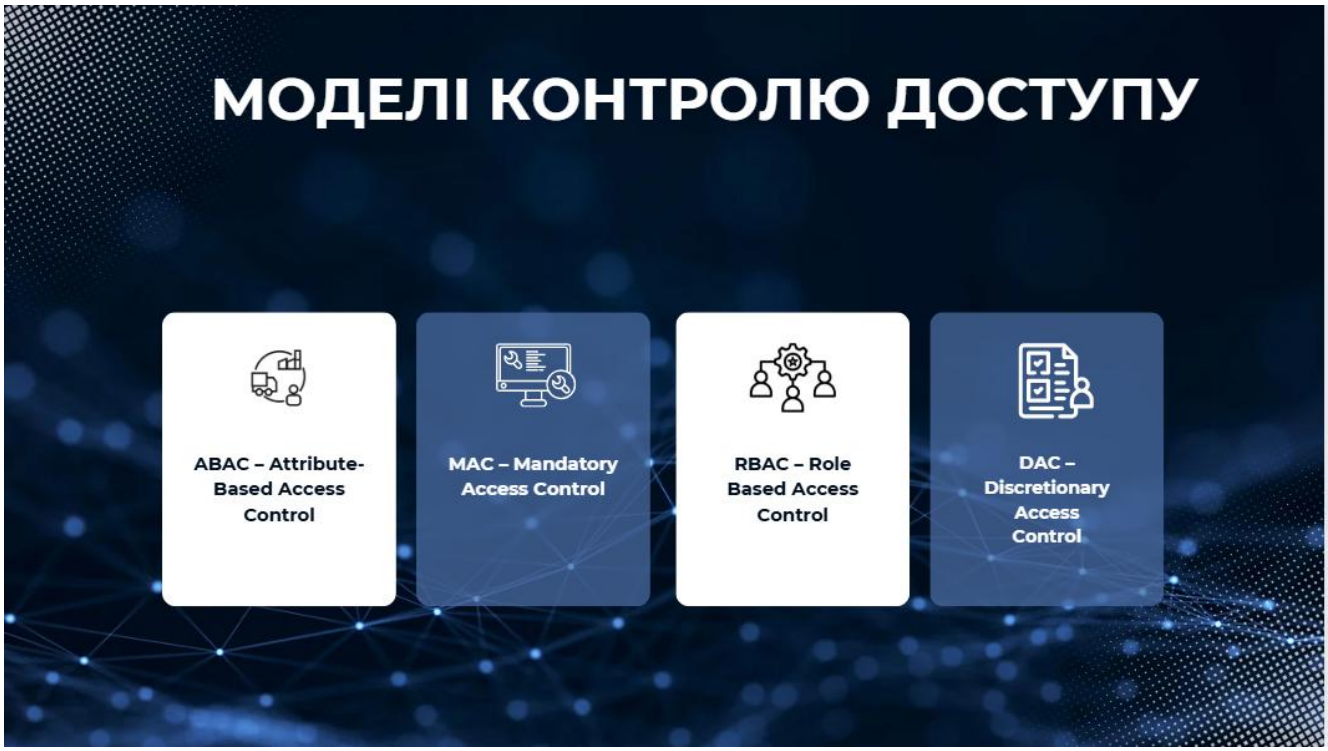
**А саме створення моделі, що забезпечить безпечне керування обліковими даними, автоматичне призначення прав доступу та контроль дій користувачів у корпоративному середовищі.**

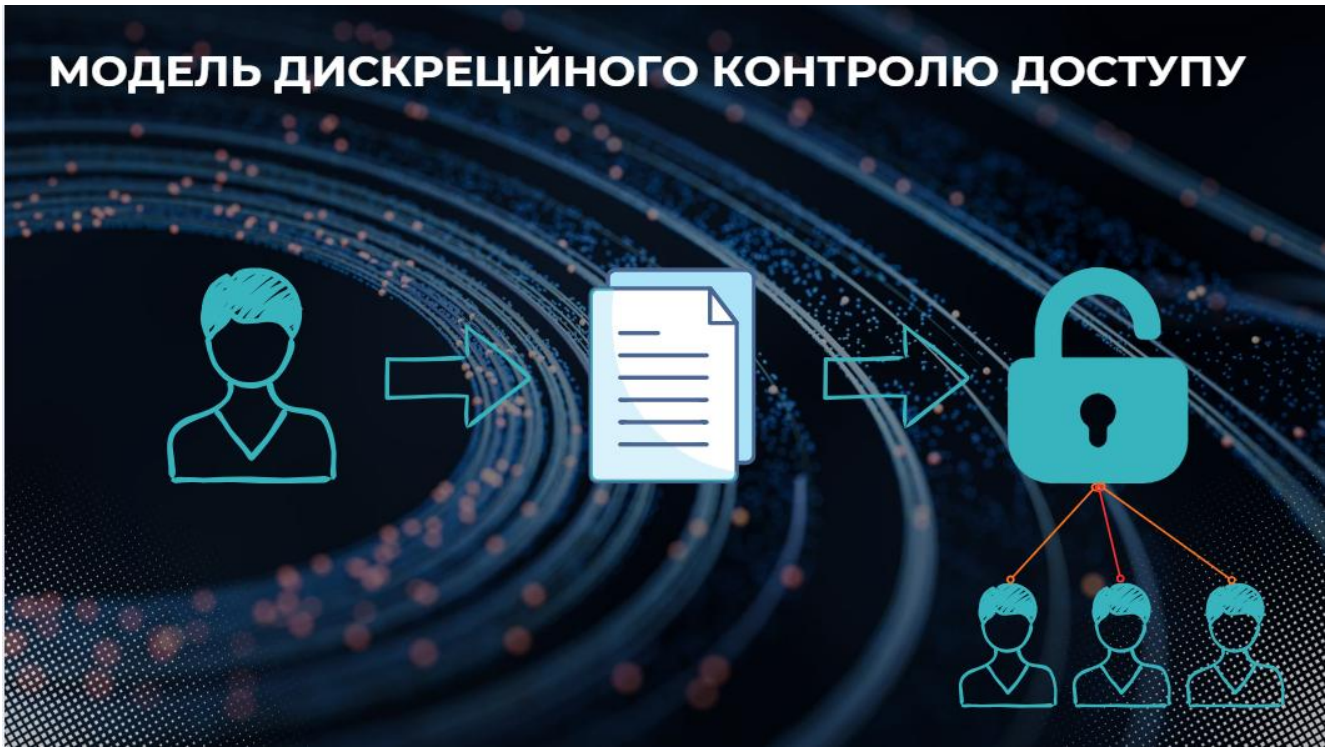
# НАУКОВА НОВИЗНА

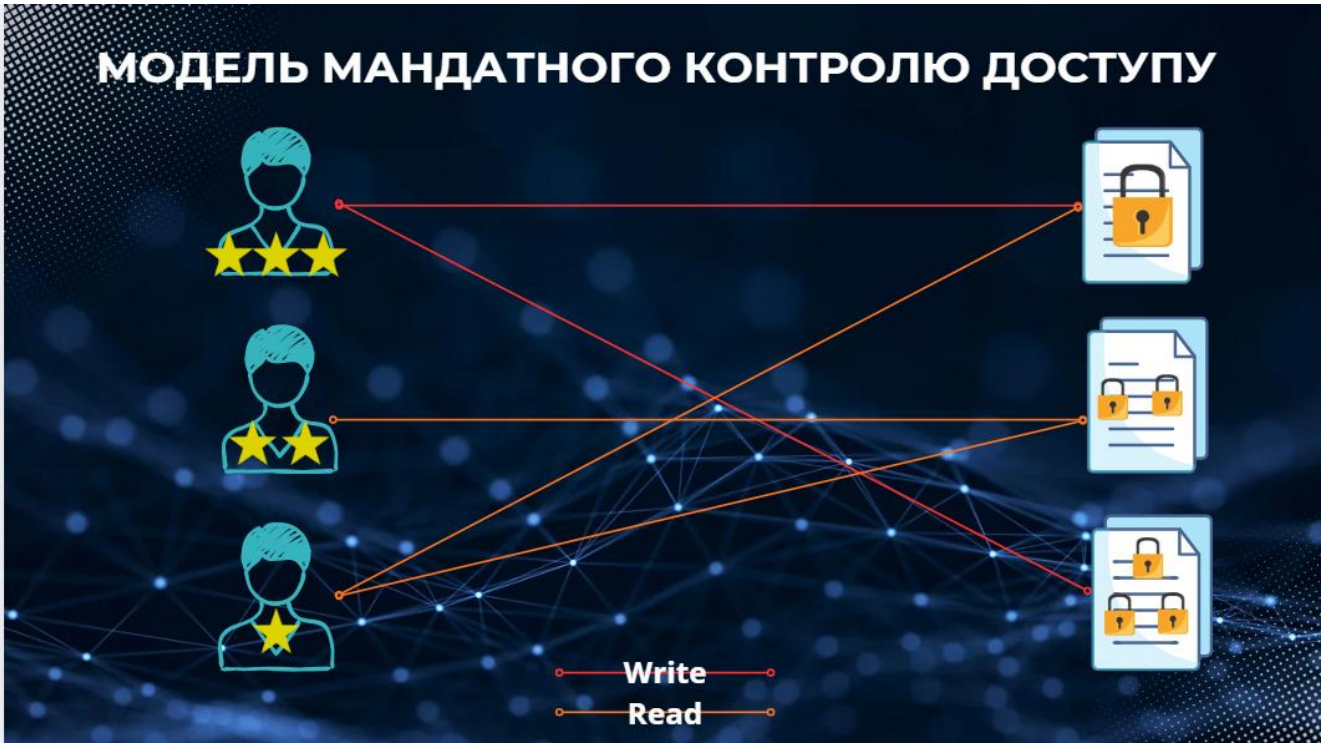
**Розроблено формалізовану модель розмежування доступу, що поєднує ролеву структуру, групові механізми та централізоване криптографічне зберігання секретів.**

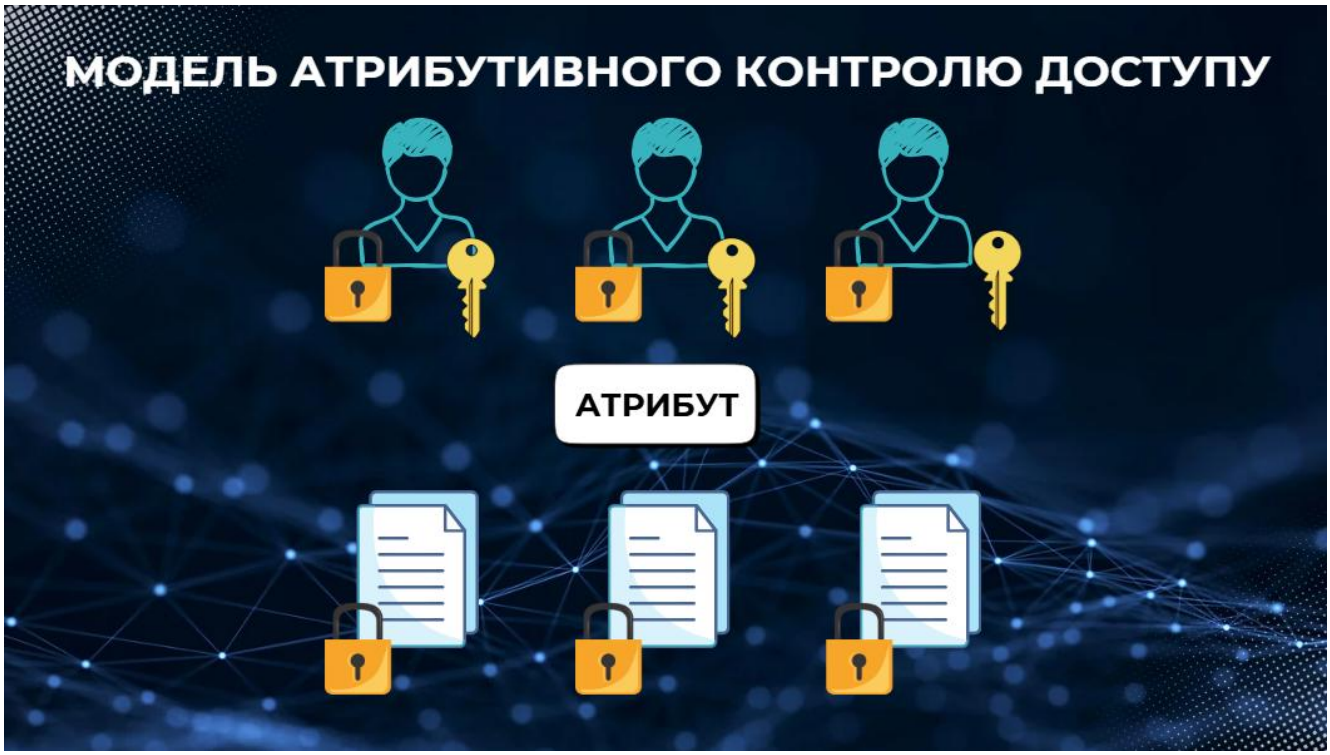
**Реалізовано інтеграцію Passbolt із корпоративним каталогом користувачів (Active Directory/LDAP) з автоматичним призначенням ролей і груп.**


ПРАКТИЧНА ЦІННІСТЬ
01
Проблема
Некеровані облікові дані. Відсутність централізованого контролю доступів
02
Рішення
Впровадження сервісу централізованого зберігання паролів за методологією інтеграції корпоративних сервісів та корп ресурсів.
03
Підвищення рівня безпеки. Прозорий контроль доступів та дій користувачів


МОДЕЛІ КОНТРОЛЮ ДОСТУПУ
ABAC – Attribute-Based Access Control
MAC – Mandatory Access Control
RBAC – Role Based Access Control
DAC – Discretionary Access Control


МОДЕЛЬ ДИСКРЕЦІЙНОГО КОНТРОЛЮ ДОСТУПУ


МОДЕЛЬ МАНДАТНОГО КОНТРОЛЮ ДОСТУПУ
Write
Read


МОДЕЛЬ АТРИБУТИВНОГО КОНТРОЛЮ ДОСТУПУ
АТРИБУТ


МОДЕЛЬ РОЛЬВОГО КОНТРОЛЮ ДОСТУПУ
Керівник
Василь
Бухгалтер
Мойша
Контора
Розробка
Владік

# ПРАКТИЧНЕ РІШЕННЯ

## Cloud (Хмарне рішення)

| Переваги | Недоліки |
|---|---|
| Швидке розгортаня | Залежність від постачальника |
| Зручність користування | Ризи компроментації |
| Оновлення та підтримка з боку постачальника | Відсутність повного контролю |

## On-Premise (Наземне рішення)

| Переваги | Недоліки |
|---|---|
| Повний контроль | Складність розгортання |
| Можливість інтеграції | Фахівці |
| Гнучкість налаштування | Ресурсоємність |

# ЛІДЕРИ НА РИНКУ ХМАРНІ РІШЕННЯ

1Password

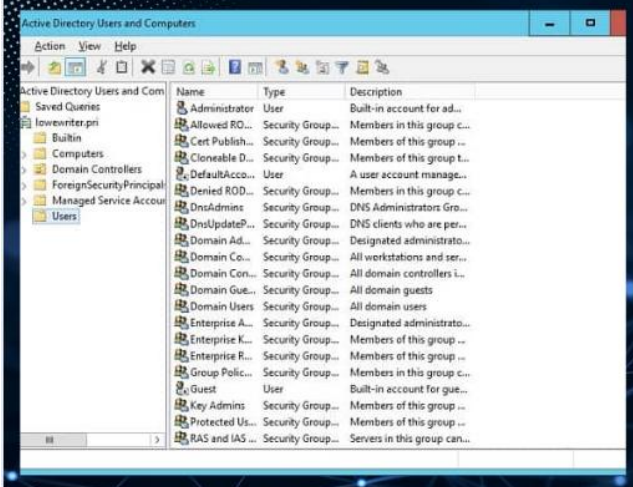
LastPass •••|

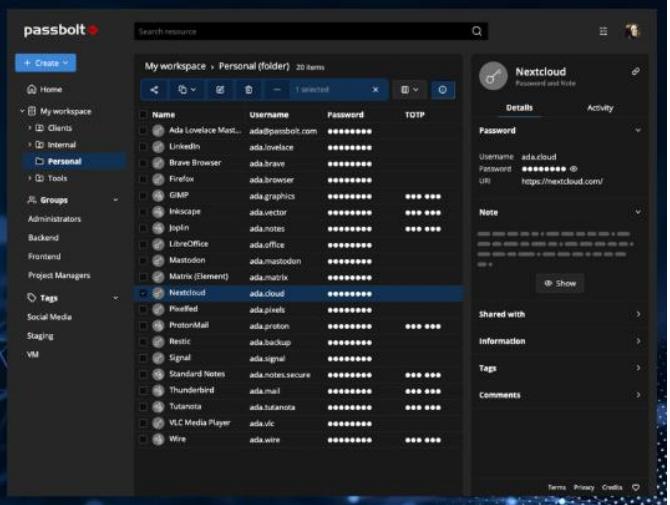
DASHLANE


## ПІДХОДИ ДО УПРАВЛІННЯ ОБЛІКОВИМИ ДАНИМИ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

| Підхід | Основна мета | Рівень складності | Приклади рішень | Орієнтація |
|---|---|---|---|---|
| IAM | Централізоване управління ідентичностями та доступом | Високий | Azure AD, Okta, Keycloak | Великі корпорації |
| PAM | Контроль привілейованих облікових записів | Високий | CyberArk | IT-відділи, DevOps |
| SSO | Єдиний вхід у кілька систем | Середній | Auth0, Keycloak, Okta | Користувачі |
| Password Vault | Безпечне зберігання та обмін паролями | Низький/середній | Passbolt, Bitwarden, KeePass | Будь-які організації |

# МОДЕЛЬ ФУНКЦІЮВАННЯ



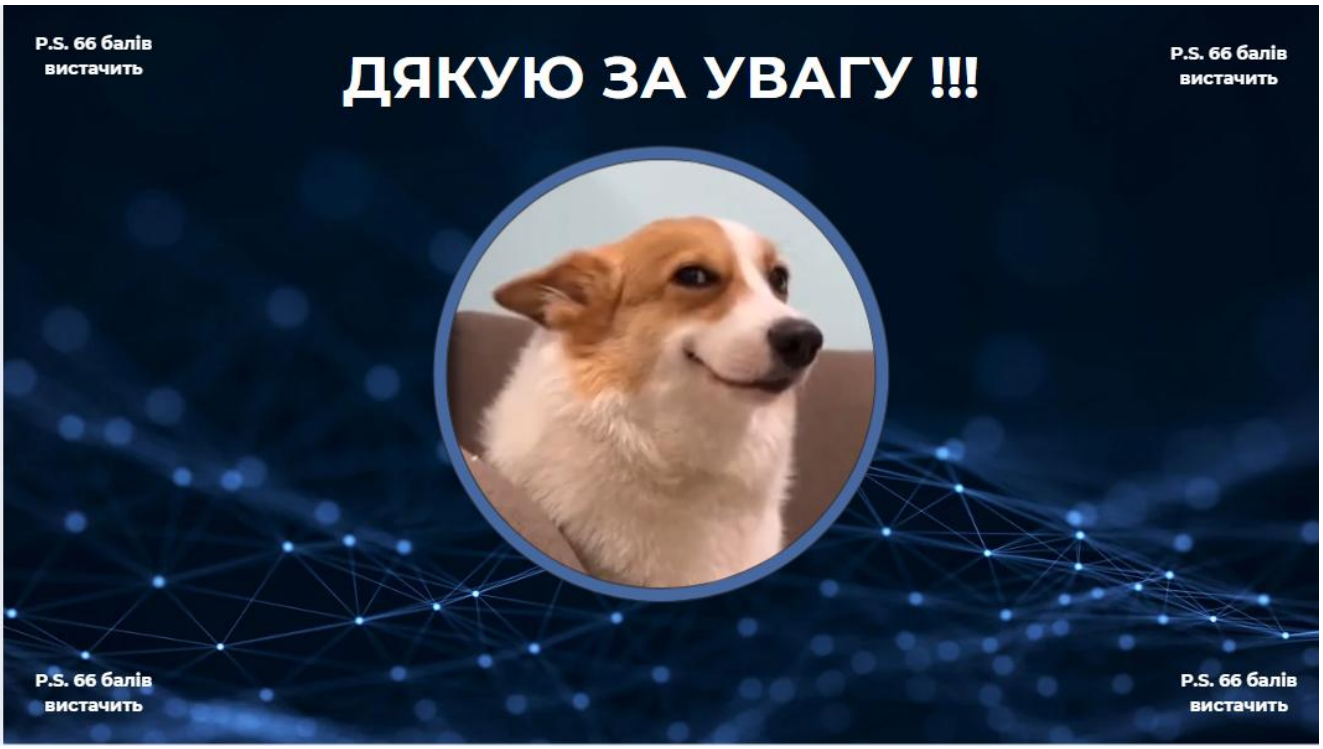




**Підключення до LDAP/AD**

```
return [
  'passbolt' => [
      'plugins' => [
          'ldap' => [
              'enabled' => true,
              'host' => 'ldap.company.local',
              'port' => 389,
              'bindDn' => 'CN=ldap_sync,OU=ServiceAccounts,DC=company,DC=local',
              'bindPassword' => 'StrongPassword123!',
              'baseDn' => 'OU=Employees,DC=company,DC=local',
              'filter' => '(objectClass=person)',
              'mapping' => [
                  'username' => 'sAMAccountName',
                  'firstname' => 'givenName',
                  'lastname' => 'sn',
                  'email' => 'mail',
              ],
          ]
      ]
  ]
];
```

**Правила відповідності OU → групам Passbolt**

```
'groupMapping' => [
  [
      'ou' => 'OU=IT,OU=Departments,DC=company,DC=local',
      'group' => 'IT-Department'
  ],
  [
      'ou' => 'OU=Support,OU=Departments,DC=company,DC=local',
      'group' => 'Support-Team'
  ],
  [
      'ou' => 'OU=Management,OU=Departments,DC=company,DC=local',
      'group' => 'Management'
  ]
],
```


P.S. 66 балів вистачить
ДЯКУЮ ЗА УВАГУ !!!
P.S. 66 балів вистачить
P.S. 66 балів вистачить
P.S. 66 балів вистачить