ТЕХНОЛОГІЯ РОЗМЕЖУВАННЯ ДОСТУП З ВИКОРИСТАННЯМ СЕРВІСУ ЦЕНТРАЛІЗОВАНОГО ЗБЕРІГАННЯ ПАРОЛЕЙ

Автор - Малінський Микита Сергійович, БІКСм-24

Керівник - Шабала Євгенія Євгеніївна

Кафедра Кібербезпеки та комп'ютерної інженерії

2025

АКТУАЛЬНІСТЬ

- Сучасні організації стикаються з ризиками через неналежне управління доступами: паролі часто зберігаються без захисту, повторно використовуються або передаються через ненадійні канали. Це підвищує ймовірність витоку даних та компрометації систем.

- Зростає кількість кібератак, націлених на викрадення облікових даних. Близько 60% інцидентів інформаційної безпеки пов’язані з неправильним налаштуванням прав доступу, слабкими паролями та відсутністю централізованого контролю.

- Покращення принципу побудови організації з дотриманням CIA - Цілістність, Конфеденційність, Доступність

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

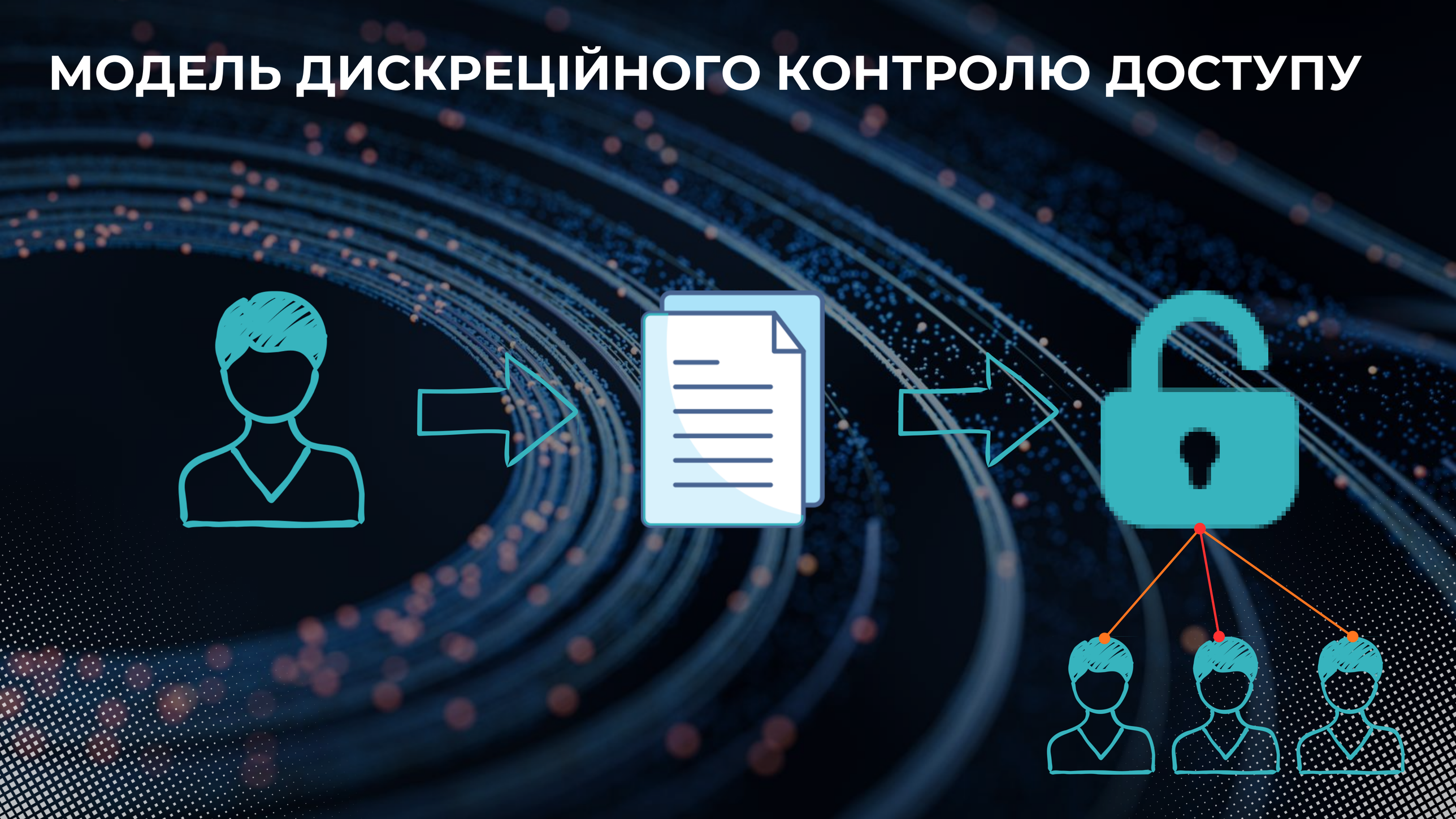
ABAC – Attribute-Based Access Control

MAC – Mandatory Access Control

RBAC – Role Based Access Control

DAC – Discretionary Access Control

МОДЕЛЬ ДИСКРЕЦІЙНОГО КОНТРОЛЮ ДОСТУПУ



МОДЕЛЬ МАНДАТНОГО КОНТРОЛЮ ДОСТУПУ

МОДЕЛЬ АТРИБУТИВНОГО КОНТРОЛЮ ДОСТУПУ

МОДЕЛЬ РОЛЬВОГО КОНТРОЛЮ ДОСТУПУ

Керівник

Васил
ь

**Контор
а**

Бухгалте
р

Мойша

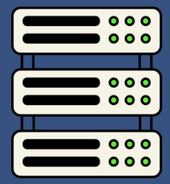
Розробка

Владі
к

ПРАКТИЧНЕ РІШЕННЯ

Cloud (Хмарне

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

ЛІДЕРИ НА РИНКУ НАЗЕМНІ РІШЕННЯ

passbolt

bitwarden

WEB-SRV

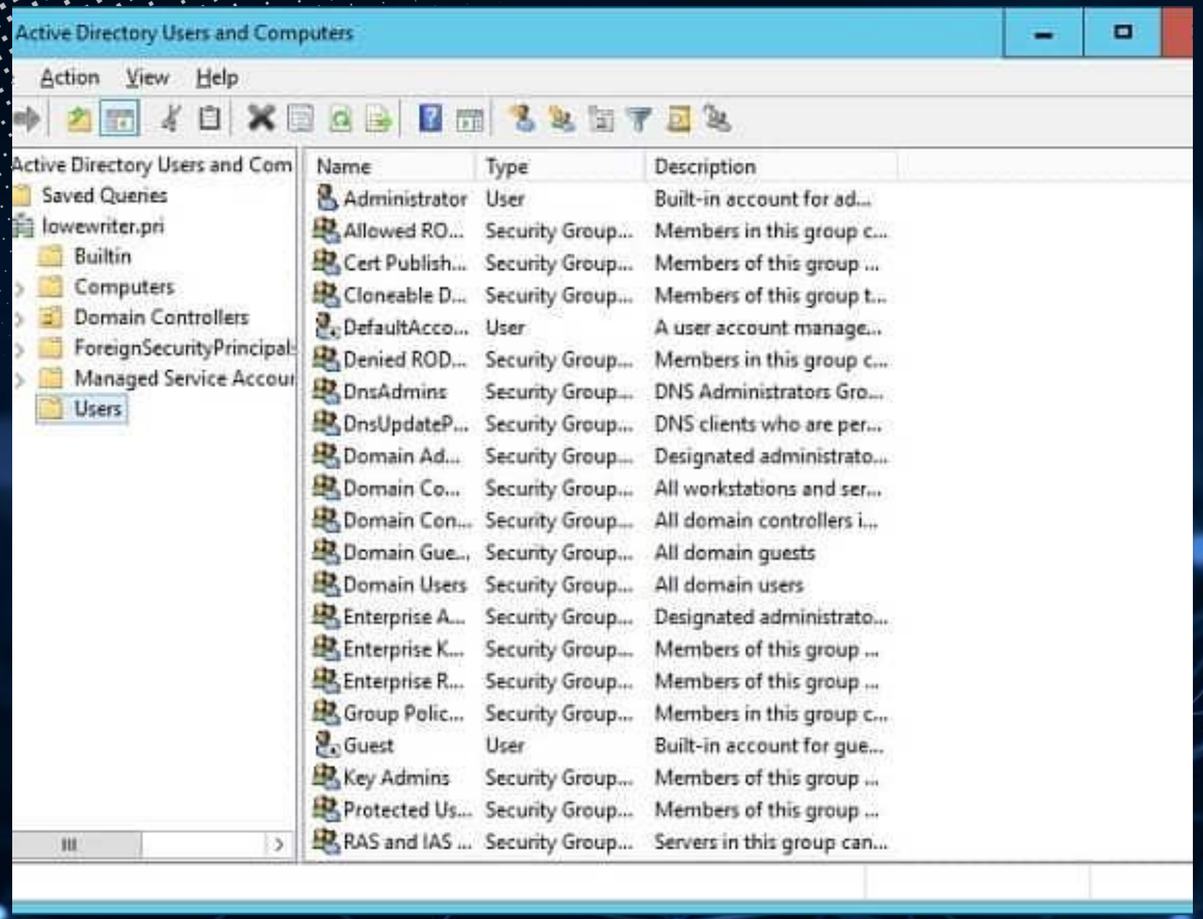
PLUGIN

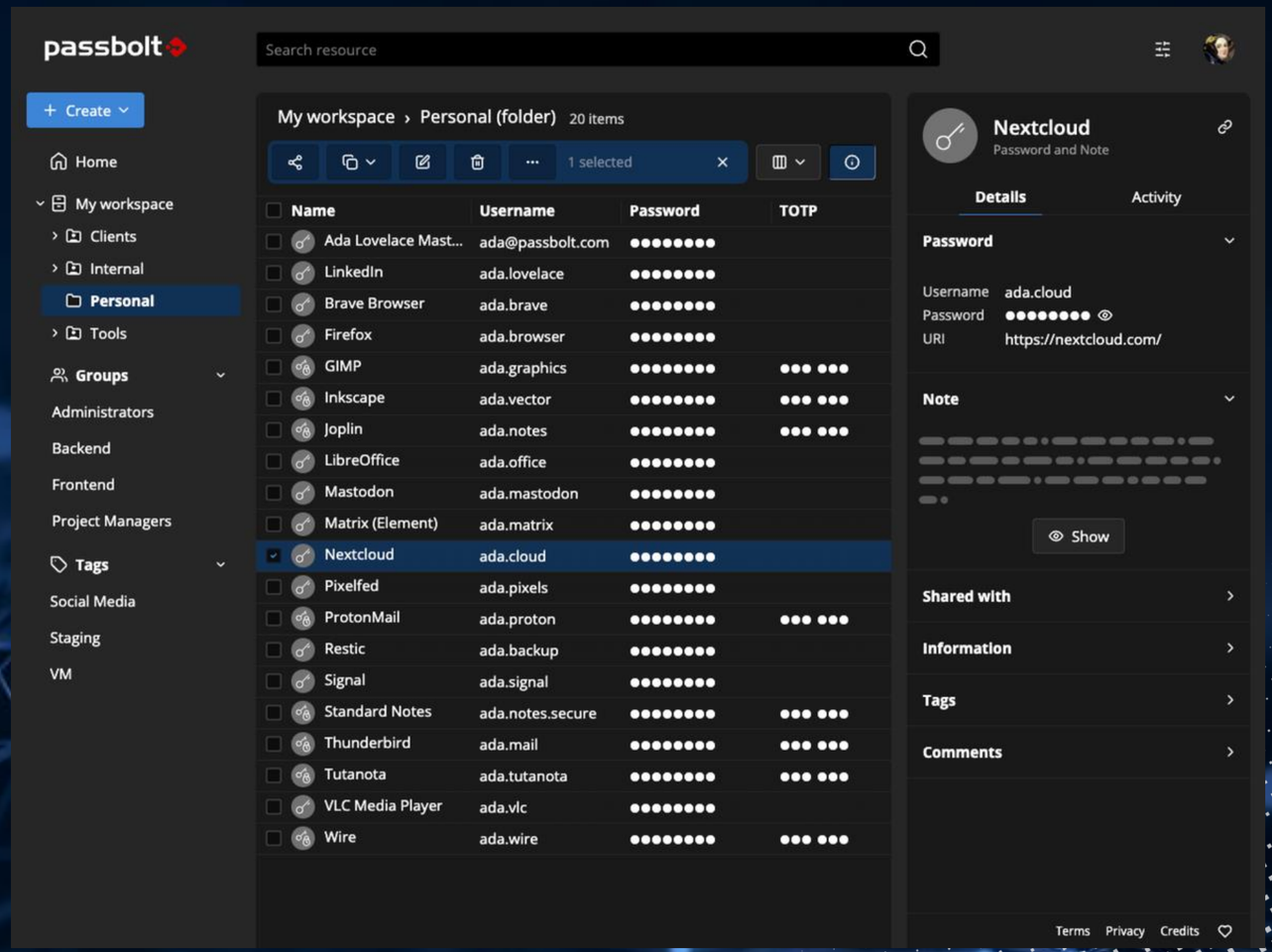
PRICE

ПІДХОДИ ДО УПРАВЛІННЯ ОБЛІКОВИМИ ДАНИМИ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Підхід	Основна мета	Рівень складності
IAM	Централізоване управління ідентичностями та доступом	Високий
PAM	Контроль привілейованих облікових записів	Високий
SSO	Єдиний вхід у кілька систем	Середній

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'
  ]
],
```

РЕЗУЛЬТАТИ

RBAC – Role Based Access Control

+

DAC – Discretionary Access Control

Password Vault

Single sign-on

Identity and Access Management

ВИСНОВКИ

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 КІБЕРЗАХИСТ

P.S. 66 балів вистачить

ДЯКУЮ ЗА УВАГУ !!!

P.S. 66 балів вистачить

P.S. 66 балів вистачить

P.S. 66 балів вистачить