

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

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 СІА - Цілісність, Конфіденційність, 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

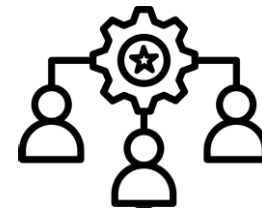
МОДЕЛІ КОНТРОЛЮ ДОСТУПУ



**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 РОЛЬОВОГО КОНТРОЛЮ ДОСТУПУ

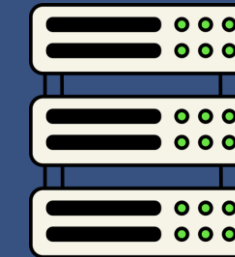


ПРАКТИЧНЕ РІШЕННЯ



Cloud (Хмарне)

Переваги	Недоліки
Швидке розгортання	Залежність від постачальника
Зручність користування	Ризи компрометації
Оновлення та підтримка з боку постачальника	Відсутність повного контролю



On-Premise (Наземне рішення)

Переваги	Недоліки
Повний контроль	Складність розгортання
Можливість інтеграції	Фахівці
Гнучкість налаштування	Ресурсоемність

ЛІДЕРИ НА РИНКУ ХМАРНІ РІШЕННЯ



1Password



LastPass

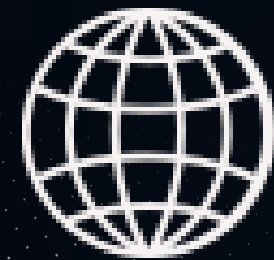


DASHLANE

ЛІДЕРИ НА РИНКУ НАЗЕМНІ РІШЕННЯ

passbolt

bitwarden



WEB-
SRV



PLUGIN



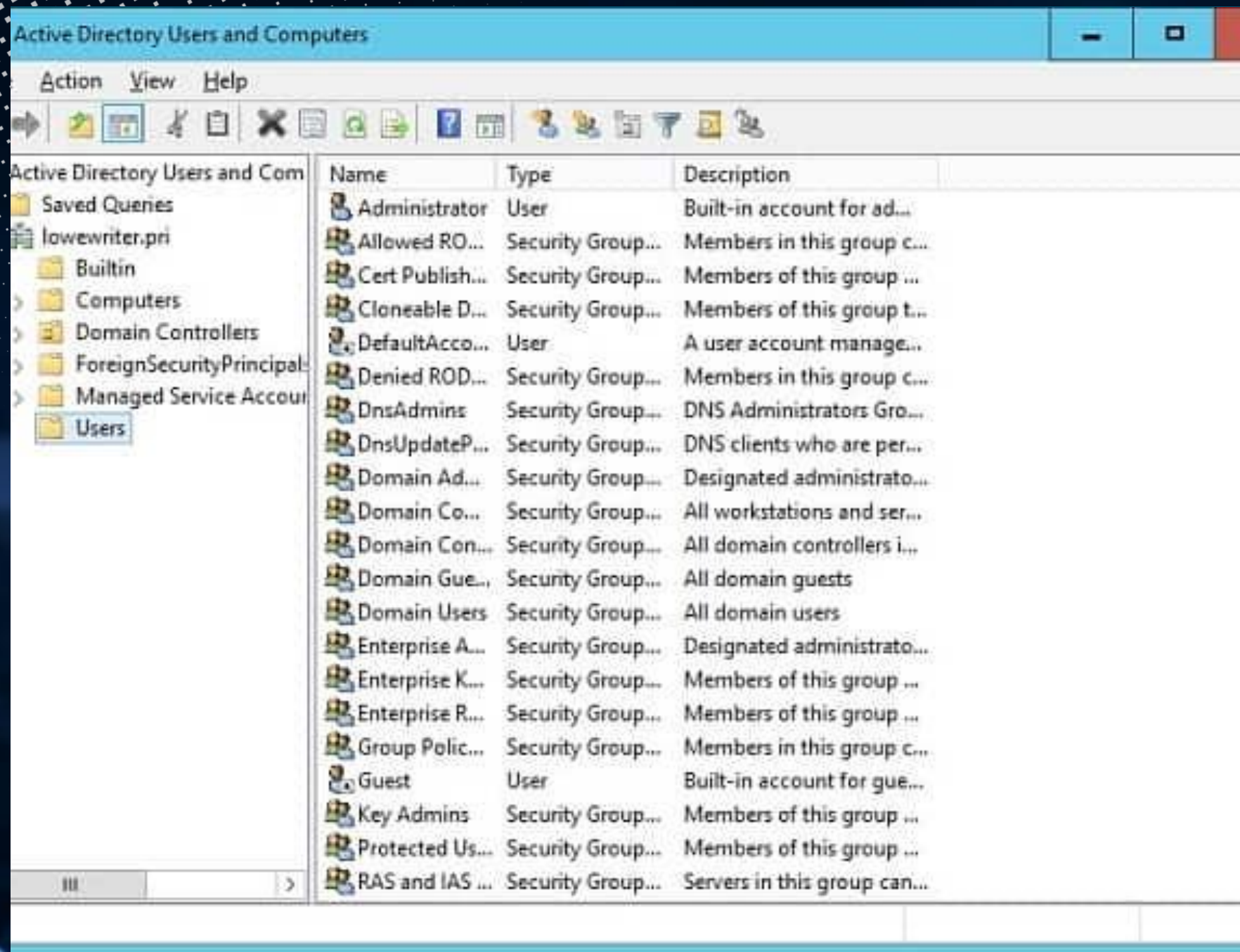
PRIC
E



ПІДХОДИ ДО УПРАВЛІННЯ ОБЛІКОВИМИ ДАНИМИ В СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

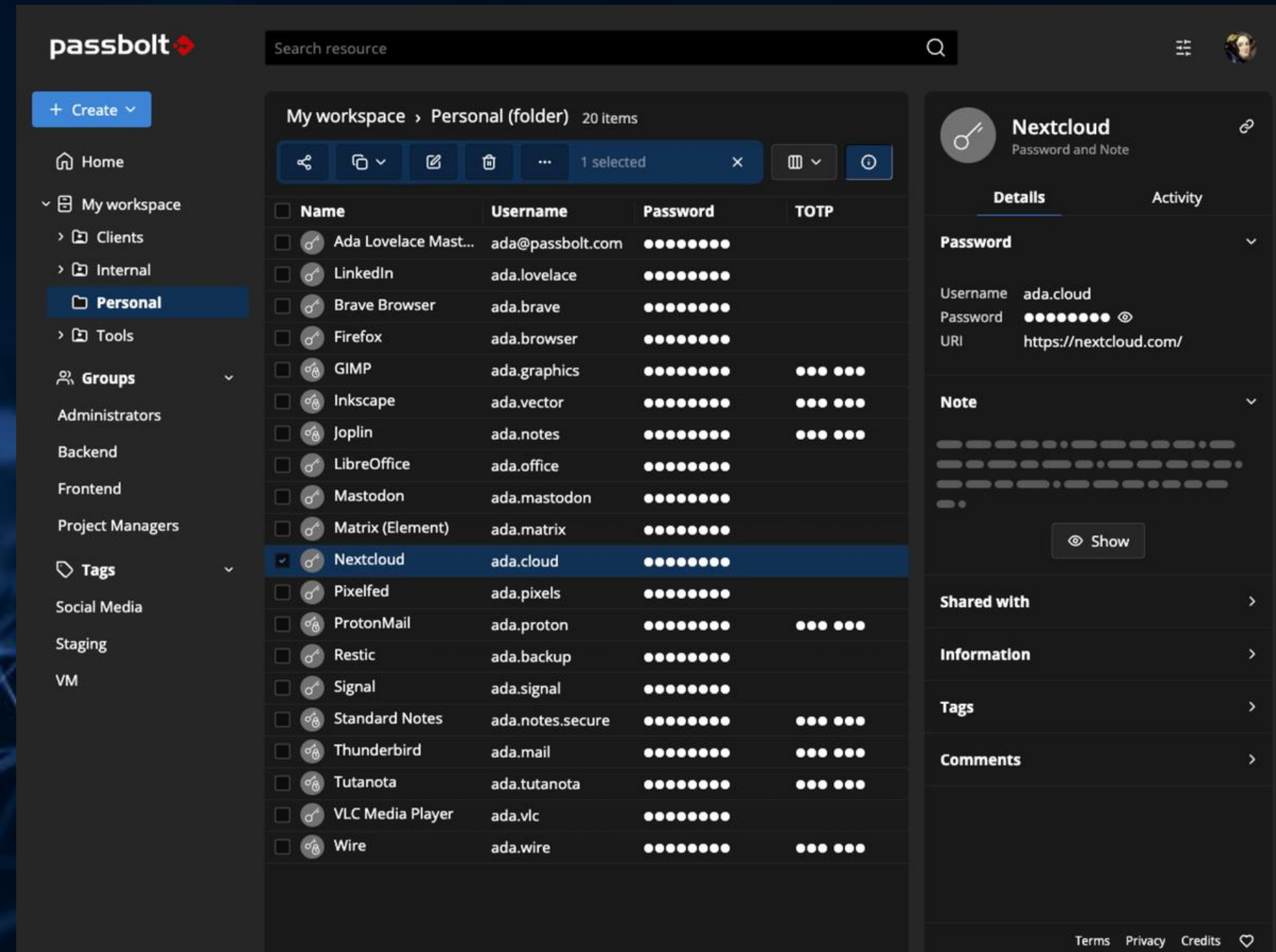
Підхід	Основна мета	Рівень складності
IAM	Централізоване управління ідентичностями та доступом	Високий
PAM	Контроль привілейованих облікових записів	Високий
SSO	Єдиний вхід у кілька систем	Середній

МОДЕЛЬ ФУНКЦІЮВАННЯ



Active Directory Users and Computers

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
DefaultAcco...	User	A user account manage...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...



passbolt

Search resource

+ Create

Home

My workspace

- Clients
- Internal
- Personal**
- Tools

Groups

- Administrators
- Backend
- Frontend
- Project Managers

Tags

- Social Media
- Staging
- VM

My workspace > Personal (folder) 20 items

Name	Username	Password	TOTP
Ada Lovelace Mast...	ada@passbolt.com	●●●●●●	
LinkedIn	ada.lovelace	●●●●●●	
Brave Browser	ada.brave	●●●●●●	
Firefox	ada.browser	●●●●●●	
GIMP	ada.graphics	●●●●●●	●●●●●●
Inkscape	ada.vector	●●●●●●	●●●●●●
Joplin	ada.notes	●●●●●●	●●●●●●
LibreOffice	ada.office	●●●●●●	
Mastodon	ada.mastodon	●●●●●●	
Matrix (Element)	ada.matrix	●●●●●●	
Nextcloud	ada.cloud	●●●●●●	
Pixelfed	ada.pixels	●●●●●●	
ProtonMail	ada.proton	●●●●●●	●●●●●●
Restic	ada.backup	●●●●●●	
Signal	ada.signal	●●●●●●	
Standard Notes	ada.notes.secure	●●●●●●	●●●●●●
Thunderbird	ada.mail	●●●●●●	●●●●●●
Tutanota	ada.tutanota	●●●●●●	●●●●●●
VLC Media Player	ada.vlc	●●●●●●	
Wire	ada.wire	●●●●●●	●●●●●●

Nextcloud
Password and Note

Details Activity

Password

Username ada.cloud
Password ●●●●●●
URI https://nextcloud.com/

Note

Show

Shared with

Information

Tags

Comments

Terms Privacy Credits

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, КЕРОВАНOSTІ
ДОСТУПІВ ТА ВІДПОВІДНОСТІ СУЧАСНИМ ВИМОГАМ
КІБЕРЗАХИСТ**

Р.С. 66 балів
ВІСТАЧИТЬ

ДЯКУЮ ЗА УВАГУ !!!

Р.С. 66 балів
ВІСТАЧИТЬ



Р.С. 66 балів
ВІСТАЧИТЬ

Р.С. 66 балів
ВІСТАЧИТЬ