УДК 004.6

Арсен ВІТВІЦЬКИЙ

Західноукраїнський національний університет

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ ТА ТЕХНОЛОГІЙ ЕФЕКТИВНОГО УПРАВЛІННЯ ПАРОЛЯМИ

Вступ. Забезпечення безпеки даних є однією із основних проблем, з якими стикаються підприємства та організації. Одним із ключових елементів безпеки є автентифікація користувачів, і паролі залишаються найбільш поширеним методом підтвердження особи. Однак зростання кіберзагроз і постійно змінювані умови безпеки вимагають впровадження ефективних інструментів і технологій для управління паролями, здатних забезпечити належний рівень захисту.

На підприємствах, де доступ до корпоративних ресурсів здійснюється через мережу, важливо мати системи, які дозволяють зберігати та обробляти паролі на належному рівні безпеки, мінімізуючи ризик їх компрометації. Інструменти для управління паролями повинні забезпечувати не лише зручність для користувачів, але й відповідати стандартам безпеки, такими як шифрування, багатофакторна автентифікація та контроль доступу.

Мета: аналіз інструментів та технологій управління паролями та розробка алгоритму автентифікації користувачів для підвищення рівня інформаційної безпеки на підприємствах.

1. Аналіз систем керування паролями

З огляду на зростаючі загрози кібербезпеки, використання системи керування паролями (СКП) (рисунок 1) стає не лише зручним, але й важливим засобом забезпечення безпеки конфіденційної інформації [1]. СКП дозволяють ефективно шифрувати облікові дані, що забезпечує їх захист від зловмисників [2]. Функції автоматичного заповнення значно спрощують використання різних сервісів. Крім того, деякі з СКП включають додаткові можливості, такі як моніторинг скомпрометованих паролів та генерація складних паролів, що дозволяє підвищити рівень захисту [3].

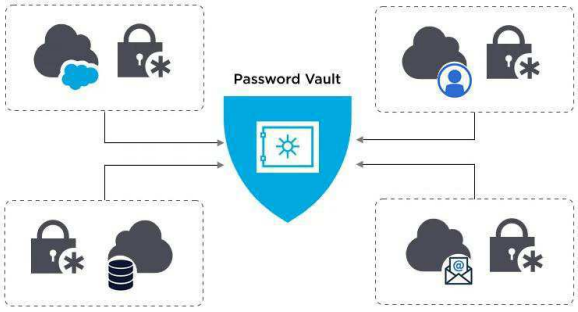

Рисунок 1 - Структура СКП

СКП є рішенням, не лише дозволяє безпечно зберігати і контролювати облікові дані, а також ділитися ними за необхідності. Серед існуючих рішень можна виділити три основні типи СКП: браузерні; спеціалізовані; вбудовані.

Більшість веб-браузерів пропонують інтегровані менеджери паролів (МП), що дозволяють створювати, зберігати та автоматично заповнювати дані, що є зручним для користувачів та не потребує додаткових налаштувань. Однак

такі МП мають обмежені можливості безпеки, оскільки є ризик несанкціонованого доступу до збережених даних, якщо пристрій потрапляє до рук сторонніх осіб.

Спеціалізовані СКП є окремими програмним додатками, які надають набагато ширший спектр функцій для зберігання та управління паролями. Вони можуть включати шифрування, синхронізацію між різними пристроями, двофакторну автентифікацію та можливість зберігання інших чутливих даних, таких як інформація про кредитні картки, документи тощо. Ці інструменти надають вищий рівень безпеки, оскільки доступ до них здійснюється лише після введення майстер-паролю, який є основним ключем для входу в цифрове сховище. Ці додатки можна встановлювати на різні пристрої та інтегрувати з веб-браузерами.

Вбудовані МП є рішеннями, які інтегровані безпосередньо в операційні системи (ОС) або пристрої. Вони забезпечують зручний доступ до паролів і синхронізують їх між пристроями в межах екосистеми, що значно спрощує користування сервісами на різних пристроях. В таблиці 1 наведено порівняльні характеристики найбільш розповсюджених МП.

Таблиця 1 - Порівняльні характеристики МП

СКП	**Хмарне сховище**	**Плагіни браузерів**
Dashlane	1-5 GB	Chrome, Firefox, Safari, Internet Explorer, Edge
NordPass	3 GB	Chrome, Firefox, Safari, Opera, Brave, Vivaldi, Edge
1Password	1-5 GB	Chrome, Brave, Firefox, Edge
Keeper	5 GB	Chrome, Firefox, Opera, Edge, Internet Explorer
Enpass	-	Chrome, Firefox, Safari, Edge, Brave, Vivaldi
RoboForm	-	Chrome, Edge, Firefox, Opera
LastPass	1 GB	Chrome, Firefox, Safari, Opera, Edge, застаріла версія Edge
RememBear	-	Chrome, Firefox и Safari
Zoho Vault	100 MB	Chrome, Firefox, Safari, Edge, Brave, Vivaldi
Passbolt	-	Chrome, Firefox
Bitwarden	1 GB	Chrome, Firefox, Vivaldi, Opera, Edge, Safari, Tor, Brave

Кожен з розглянутих МП має свої переваги та недоліки. Браузерні МП пропонують зручність і інтеграцію в екосистему певних пристроїв чи програм, але не забезпечують такого рівня безпеки, як спеціалізовані МП. Спеціалізовані СКП забезпечують більший рівень захисту, адже часто використовують механізми шифрування, які гарантують, що тільки авторизовані користувачі мають доступ до своїх облікових даних. Крім того, при використанні МП з принципом нульового розкриття, навіть адміністратор, який відповідає за СКП, не має доступу до збережених даних. Мультиплатформна сумісність таких СКП забезпечує доступ до паролів з будь-якого пристрою чи місця, за умови наявності відповідного додатка або розширення для браузера. Спеціалізовані МП також оснащені функцією безпечного обміну даними, яка гарантує, що передача інформації відбувається лише в зашифрованому вигляді, що значно знижує ризик стороннього доступу під час обміну конфіденційною інформацією.

2. Розробка алгоритму автентифікації користувачів спеціалізованиї системи керування пололями

Проведений аналіз дозволилив визначити функції (рисунок 2) та характеристики, які впливають на безпеку та ефективність СКП, зокрема:

1. Шифрування з використанням надійних алгоритмів шифрування для захисту паролів від несанкціонованого доступу.

2. Майстер-пароль, як єдиний засіб, що забезпечує доступ до всіх збережених облікових даних і необхідність його надійності.

3. Мультиплатформна сумісність для забезпечення підтримки різних пристроїв та ОС для отримання доступу до паролів, що підвищує зручність і мобільність користувачів.

4. Багатофакторна автентифікація, завдяки інтеграції додаткових рівнів захисту дозволяє підвищити рівень захисту облікових даних.

5. Автозаповнення та генерація паролів дозволяє автоматизувати процес заповнення форм автентифікації та створювати складні паролі для запобігання використанню слабких або повторюваних паролів.

6. Безпечний обмін даними забезпечує можливість обміну не лише паролями, а й іншою конфіденційною інформацією між користувачами за допомогою шифрування.

7. Керування доступом - механізми управління доступом, включаючи рольові моделі та обмеження доступу до паролів в залежності від прав користувача, для запобігання зловживанням.

8. Моніторинг скомпрометованих паролів забезпечує можливість перевірки паролів на наявність у базах даних (БД) компрометованих паролів для їх зміни.

9. Інтеграція з іншими системами безпеки, наприклад системами виявлення вторгнень (IDS) або централізовані системи управління доступом (IAM).

10. Простота використання та інтуїтивно зрозумілий інтерфейс з для забезпечення швидкого освоєння і ефективного використання СКП кінцевими користувачами.

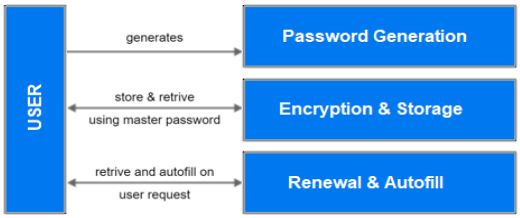

Рисунок 2 - Функції СКП

Для реалізації перелічених функцій розроблено алгоритми роботи СКП, що включають такі етапи: реєстрація користувачів, автентифікація та оновлення даних. Механізм безпеки включають хешування паролів з використанням надійного криптографічного хеш-алгоритму та шифрування даних за допомогою асиметричного шифрування для захисту хешів.

Алгоритм автентифікації (рисунок 3) включає наступні кроки:

- введення даних: ім'я та пароль користувача;
- перевірка існування імені користувача в базі даних (БД), що включає збережену інформацію про користувачів, зокрема унікальний ID, що відповідає імені користувача, зашищений хеш пароля, сіль для хешування. Якщо ні, вивести

повідомлення про помилку. Якщо так, продовжити роботу.

- отримання зашифрованого хешу та солі для користувача з БД;
- дешифрування хешу пароля - збережений хеш пароля розшифровується за допомогою приватного ключа RSA;
- перевірка введеного пароля - дані хешуються з тією ж сіллю, що зберігається в БД, і результат порівнюється з розшифрованим хешем пароля. Якщо дані співпадають, автентифікація успішна.

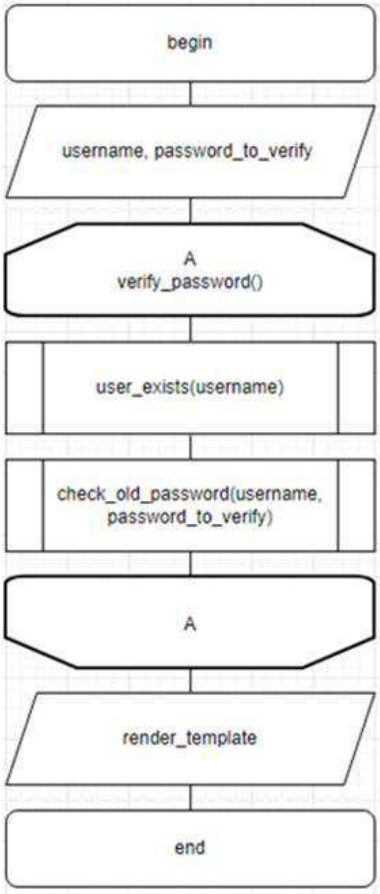

Рисунок 3 - Алгоритм автентифікації

Висновок. Запропонований алгоритм може бути використаний в спеціалізований системі керування паролями, яка забезпечує надійний захист завдяки комбінуванню RSA та хешування з сіллю. Це мінімізує ризики розкриття паролів, оскільки навіть при перехопленні даних неможливо відновити їх початковий вигляд. Використання різних криптографічних методів гарантує комплексний підхід до захисту даних, забезпечуючи конфіденційність, цілісність та доступність інформації в процесі її збереження та передачі.

Перелік використаних джерел.

1. Інформаційна безпека / за заг. ред. Ю.Я. Бобала та І.В. Горбатого / Львів: Видавництво Львівської політехніки, 2019. 580 с.
2. Скітер І., Ворохоб М. Модель оцінки рівня культури кібербезпеки в інформаційній системі.- Кібербезпека: освіта, наука, техніка. Том 1, № 13.-2021.- с. 158- 169. https://doi.org/10.28925/2663-4023.2021.13.158169.
3. Nehme A., Li M., Warkentin M. Adaptive and Maladaptive Factors behind Password Manager Use: A Hope-Extended Protection Motivation Perspective. Computers Security. 144. 2024. https://doi.org/10.1016/j.cose.2024.103941.