МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

ВІТВІЦЬКИЙ Арсен Олександрович

Спеціалізована система керування паролями доступу до ресурсів підприємств / A Specialized Password Management System for Access to Enterprise Resources

спеціальність: 125 – Кібербезпека та захист інформації

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм - 21
А.О. Вітвіцький

_____

Науковий керівник
С.В.Івасьєв

_____

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2024 р.

Завідувач кафедри

_____ **В.В.Яцків**

ТЕРНОПІЛЬ – 2024

Факультет комп'ютерних інформаційних технологій

Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 20___ року

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

ВІТВІЦЬКИЙ Арсен Олександрович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Спеціалізована система керування паролями доступу до ресурсів підприємств / A Specialized Password Management System for Access to Enterprise Resources
керівник роботи С.В. Івасьєв

затверджені наказом по університету від 12 грудня 2023 року № 753

2. Строк подання студентом закінченої кваліфікаційної роботи 12 грудня 2024 року.
3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:
– проаналізувати характеристики існуючих інструментів управління паролями;
– проаналізувати методи шифрування, які використовуються в системах управління паролями, та вимоги до їх безпеки;
– дослідити алгоритми роботи менеджера паролів;
– дослідити потенційні вразливості в системах управління паролями;
– розробити спеціалізовану систему управління паролями для підприємства з використанням сучасних криптографічних алгоритмів.
5. Перелік графічного матеріалу у роботі.
– структура спеціалізованої системи керування паролями;
– алгоритм реєстрації;
– алгоритм автентифікації;
– алгоритм оновлення даних.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 12 грудня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз інструментів та технологій керування паролями	12.2023 р. – 03.2024 р.	
2	Дослідження вразливостей та алгоритмів роботи систем управління паролями	03.2024 р. – 06.2024 р.	
3	Реалізація спеціалізованої системи керування паролями	06.2024 р. – 11.2024 р.	

Студент _____ А.О. Вітвіцький
(підпис)

Керівник роботи _____ С.В. Івасьєв
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Спеціалізована система керування паролями доступу до ресурсів підприємств» на здобуття освітнього ступеня «Магістр» зі спеціальності 125 «Кібербезпека та захист інформації» освітньо-професійної програми «Кібербезпека» написана обсягом 62 сторінках і містить 33 ілюстрації, 1 таблицю, 3 додатки та 36 джерел за переліком посилань.

Метою роботи є дослідження дослідження систем управління паролями щодо їх ефективності та безпеки та розробка спеціалізованого рішення для оптимізації процесу автентифікації, що забезпечує надійний захист облікових даних від кіберзагроз.

Методи досліджень. Для розв'язання поставлених задач використано методи аналізу систем управління паролями, порівняльний аналіз існуючих інструментів і технологій управління паролями, експериментальне дослідження для виявлення вразливостей у системах управління паролями, методи моделювання для розробки спеціалізованої системи керування паролями до ресурсів підприємств.

Результати дослідження: розробка спеціалізованої системи управління паролями, що оптимізує процес автентифікації, забезпечуючи надійний захист облікових даних від несанкціонованого доступу. Визначено ефективні методи шифрування та управління паролями, які підвищують загальний рівень безпеки інформаційних систем підприємств.

Запропоновані рішення можуть бути впроваджені в системах управління паролями для підвищення безпеки облікових даних, а також в інших сферах, де необхідний високий рівень захисту, зокрема в корпоративних інформаційних системах та фінансових сервісах.

Ключові слова: КЕРУВАННЯ ПАРОЛЯМИ, ІНФОРМАЦІЙНА БЕЗПЕКА, АВТЕНТИФІКАЦІЯ, ВРАЗЛИВОСТІ, КРИПТОГРАФІЧНІ АЛГОРИТМИ.

ABSTRACT

Qualification work on " A Specialized Password Management System for Access to Enterprise Resources " for the degree of "Master" in the specialty 125 "Cybersecurity and Information Protection" educational and professional program "Cybersecurity" is written in 62 pages and contains 33 illustrations, 1 table, 3 appendices and 36 source according to the list of links.

The aim of this work is to investigate password management systems in terms of their effectiveness and security, and to develop a specialized solution for optimizing the authentication process that ensures reliable protection of credentials against cyber threats.

Research methods. To address the tasks set, methods of analyzing password management systems were used, comparative analysis of existing tools and technologies for password management, experimental research to identify vulnerabilities in password management systems, and modeling methods for developing a specialized password management system for enterprise resources.

Research results: The development of a specialized password management system that optimizes the authentication process while providing reliable protection of credentials against unauthorized access has been undertaken. Effective encryption and password management methods have been identified, enhancing the overall security level of enterprise information systems.

The proposed solutions can be implemented in password management systems to enhance the security of credentials, as well as in other areas where a high level of protection is required, particularly in corporate information systems and financial services.

Keywords: PASSWORD MANAGEMENT, INFORMATION SECURITY, AUTHENTICATION, VULNERABILITIES, CRYPTOGRAPHIC ALGORITHMS.

ЗМІСТ

Перелік умовних скорочень 6
Вступ 7
1. Аналіз інструментів та технологій керування паролями 10
1.1 Класифікація менеджерів паролів 10
1.2 Існуючі інструменти управління паролями 12
1.3 Методи шифрування в системах керування паролями 24
1.4 Вимоги до безпечних інструментів керування паролями 26
2 Дослідження вразливостей та алгоритмів роботи систем управління паролями 28
2.1 Керування паролями доступу до ресурсів підприємства 28
2.2 Алгоритми роботи менеджера паролів 30
2.2.1 Алгоритм зберігання та управління обліковими даними 30
2.2.2 Алгоритми реєстрації та автентифікації користувача 32
2.2.3 Алгоритм створення та редагування пароля 33
2.2.4 Алгоритм отримання пароля з сервера 36
2.3 Вразливості в системах керування паролями 37
3. Розробка спеціалізованої системи керування паролями 41
3.1 Структура системи керування паролями підприємства 41
3.2 Алгоритм роботи проектованої системи 43
3.3 Реалізація системи керування паролями 51
Висновки 58
Перелік використаних джерел 59
ДОДАКТОК А Програмна реалізація серверної частини 63
ДОДАТОК Б Програмна реалізація інтерфейсу користувача 69
ДОДАТОК В Копії публікацій 73

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СКП - система керування паролями;

МП - мереджер паролів;

НД - несанкціонований доступ;

2ФА - двофакторна автентифікація;

ВФА - багатофакторна автентифікація;

БД - база даних;

ПЗ - програмне забезпеченя;

ТОП - тимчасовий одноразовий пароль.

ВСТУП

Актуальність теми. На даний час тенденції та обставини сприяють тому, що віддалена робота стає невід'ємною частиною організації бізнес-процесів [1-3]. Значна кількість підприємств переходить на дистанційний формат роботи, тому виникає необхідність забезпечення віддаленого доступу до корпоративних ресурсів та використання спеціалізованих додатків для підтримки ефективної взаємодії й виконання робіт. Це, в свою чергу, вимагає впровадження заходів для забезпечення безпеки даних, оскільки віддалений доступ до ресурсів підвищує ризик кіберзагроз [4-6]. Одним із ключових аспектів забезпечення інформаційної безпеки в таких усмовах є управління паролями, оскільки автентифікація за допомогою пароля залишається найбільш поширеним і доступним методом підтвердження особи.

Незважаючи на досягнення в галузі дослідження безпеки, паролі продовжують залишатися вразливим місцем через людський фактор та недостатню захищеність систем [7-9]. Основні проблеми включають використання слабких або однакових паролів для різних сервісів, відсутність належної дисципліни у створенні та зберіганні паролів, а також вразливості самих інформаційних систем [10]. Такі системи стають легкою мішенню для зловмисників, які можуть здійснювати атаки, використовуючи скомпрометовані паролі. Тому актуальною задачею є розробка та впровадження спеціалізованих систем керування паролями, які допоможуть підприємствам ефективно контролювати доступ до своїх ресурсів, знижуючи ризики компрометації даних [11-13].

Такі системи призначені забезпечити надійний захист паролів, регулярні оновлення та моніторинг безпеки, а також сприяти дотриманню сучасних стандартів у галузі кібербезпеки. Використання сучасних криптографічних методів, таких як хешування з додаванням солі та асиметричне шифрування, ускладнює злам облікових даних у таких системах. Це гарантує, що для кожного відкритого пароля існує безліч

відповідних значень, що вимагає складних обчислень для потенційних атак.

Мета і завдання дослідження. Метою дослідження є розробка спеціалізованої системи керування паролями для забезпечення надійного та безпечного доступу до ресурсів підприємств.

Відповідно до мети кваліфікаційної, передбачено вирішити завдання:

- провести аналіз інструментів та засобів керування паролями;
- проаналізувати риптографічні методи, що використовуються для захисту паролів;
- дослідити вразливості в існуючих системах управління паролями та методи їх усунення;
- дослідити алгоритмів роботи систем управління паролями;
- розробити систему керування паролями.

Об'єкт дослідження – процеси управління паролями.

Предмет дослідження – методи та інструменти керування паролями для забезпечення безпечного доступу до ресурсів підприємств.

Методи досліджень. Аналіз літературних джерел та технічної документації для дослідження існуючих систем управління паролями, криптографічних методів захисту та вразливостей; порівняльний аналіз з метою оцінки ефективності та безпеки різних інструментів і засобів керування паролями; моделювання для вивчення алгоритмів шифрування та автентифікації у системах управління паролями; експериментальні дослідження для тестування розробленої системи керування паролями в умовах реального використання; методи системного аналізу для виявлення та оцінки можливих вразливостей систем управління паролями та побудови заходів для їх усунення.

Наукова новизна отриманих результатів. Розроблена система керування паролями забезпечує захищене зберігання та динамічне управління обліковими даними. Запропоновано використання хеш-функцій у поєднанні з генерацією солі, що ускладнює атаки, орієнтовані на злам паролів. Застосування асиметричного алгоритму для шифрування результатів

хешування паролів з сіллю забезпечує додатковий рівень безпеки. Система дозволяє легко масштабувати процеси управління паролями, включаючи механізми логування та моніторингу, що дозволяє проводити подальший аналіз безпеки та виявлення аномалій у поведінці користувачів.

Практичне значення отриманих результатів. Запропонована систем керування паролями доступу до ресурсів є комплексним рішенням, що дозволяє забезпечити безпеку облікових записів шляхом хешування даних з сілля, безпечне зберігання паролів за рахунок використання асиметричного шифрування. Система характеризується гнучкістю, ефективністю і зручністю використання та може бути інтегрована в існуючі системи підприємства.

Публікації та апробація кваліфікаційної роботи.

1. Вітвіцький А.О. Дослідження інструментів та технологій ефективного управління паролями / Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2024), Тернопіль, 2024. - с 27-30.

2. Вітвіцький А. Гавришків Н., Кульчинська Н. Дослідження вразливостей систем керування паролями / Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - с. 101-104.

1 АНАЛІЗ ІНСТРУМЕНТІВ ТА ТЕХНОЛОГІЙ КЕРУВАННЯ ПАРОЛЯМИ

1.1 Класифікація менеджерів паролів

З огляду на зростаючі загрози кібербезпеки, використання системи керування паролями (СКП) стає не лише зручним, але й критично важливим [4-9]. Вони забезпечують шифрування паролів, що захищає їх від зловмисників, а також функції автоматичного заповнення, що значно спрощують користування різними сервісами. Окрім того, деякі з них пропонують додаткові можливості, такі як моніторинг скомпрометованих паролів і генерація складних паролів, що ще більше підвищує рівень безпеки [11-13]. Таким чином, вибір правильного менеджера облікових даних є не лише питанням зручності, а й важливий крок у захисті конфіденційних даних [14].

СКП це корисне рішення, яке дозволяє користувачам безпечно зберігати, контролювати свої облікові дані та ділитися ними за необхідності. Деякі мереджери паролів (МП) також підтримують зберігання додаткових даних, таких як ключі доступу, документи, файли та зображення, забезпечуючи комплексний захист інформації [15]. Серед СКП виділити три основні види, зокрема браузерні, спеціалізовані та вбудовані. Веб-браузери, як Google Chrome, Mozilla Firefox, Safari та Microsoft Edge, мають вбудовані МП. Вони допомагають користувачам створювати, зберігати та автоматично заповнювати паролі. Дані МП є зручними оскільки працюють без додаткових налаштувань. Проте вони мають обмежені можливості безпеки через можливість несанкціонованого доступу (НД), якщо пристрій потрапляє до рук третіх осіб. Браузерні МП дозволяють отримувати доступ до збережених паролів лише з відповідного браузера.

Спеціалізовані системи управління паролями - це окремі програмні додатки, які пропонують широкий спектр функцій для зберігання та управління паролями. Вони часто включають додаткові можливості, такі як

шифрування, синхронізація між пристроями, двофакторна автентифікація (2ФА) та можливість зберігання інших конфіденційних даних, наприклад інформації про кредитні картки, документи тощо [16]. Такі МП допомагають створювати надійні паролі, а також безпечно їх зберігати, автоматично заповнювати та передавати. Багато з цих менеджерів можуть зберігати не лише паролі, а й ключі доступу, коди 2ФА, зображення, файли та документи. Вони забезпечують значно виший рівень безпеки, оскільки для доступу до них потрібен майстер-пароль, який є ключем для входу в цифрове сховище паролів. Крім того, вони дозволяють включити 2ФА для додаткового захисту сховища та запобігання НД. Додатки для спеціалізованих МП також можна завантажити на різні пристрої, а їх розширення в різні веб-браузери. До числа таких МП належать Keeper [17], Dashlane [18] та 1Password [19].

Вбудовані МП є рішеннями, які інтегровані в операційні системи (OS) або пристрої. Вони забезпечують зручний доступ до паролів та синхронізують їх між пристроями в межах екосистеми. Прикладом такого МП є зв'язка ключів iCloud на iPhone [20]. Ця МП пропонує користувачам можливість створювати, зберігати та автоматично заповнювати паролі, а також безпечно ділитися ними з іншими користувачами Apple за допомогою функції Airdrop.

Кожен тип менеджера облікових даних має свої переваги та недоліки. Проте браузерні МП і зв’язка ключів iCloud не забезпечують такого рівня безпеки як спеціалізовані МП, що забезпечують більш надійний захист. При використанні МП з нульовим розкриттям навіть адміністратор, що відповідає за управління паролями, не має доступу до збережених даних. Мультиплатформна сумісність забезпечує доступ до інформації з будь-якого місця і пристрою, при умові, що встановлений відповідний додаток або розширення для браузера. Спеціалізовані МП оснащені функцією безпечного обміну даними, яка гарантує, що інформація буде зашифрована при відправці отримувачу.

1.2 Існуючі інструменти управління паролями

Сервіс управління доступом Keeper [17] відомий надійними протоколами безпеки та інтуїтивним інтерфейсом (рисунок 1.1). Його підхід з нульовим розголошенням забезпечує шифрування даних на пристроях до їх відправки на сервер. Keeper підтримує 2ФА, включаючи біометричну автентифікацію та сумісний з усіма основними платформами та браузерами.

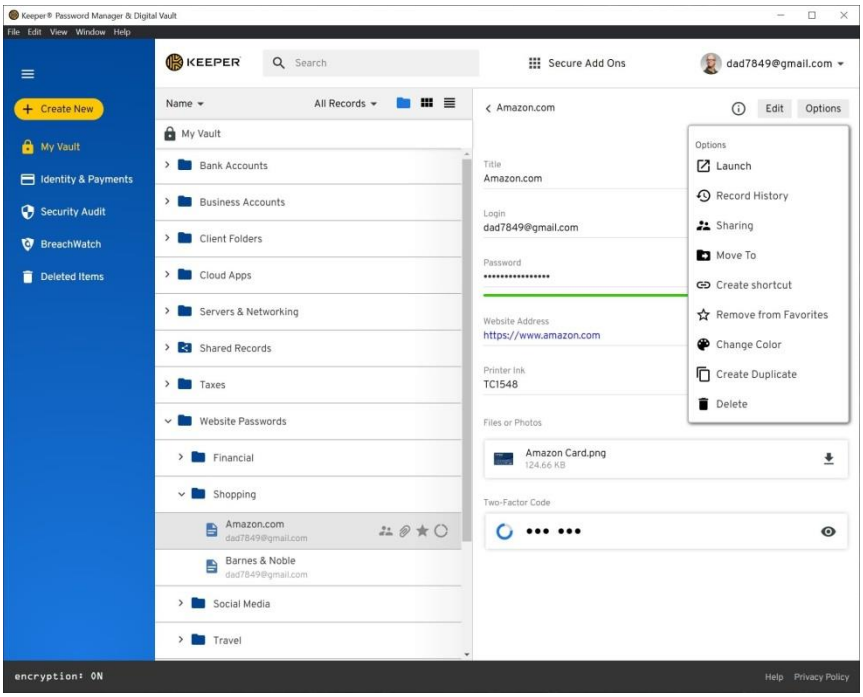


Рисунок 1.1 – Keeper

Перевагами даного МП є широка сумісність, безпечний обмін повідомленнями, різні варіанти 2ФА. Серед недоліків можна виділити відсутність безкоштовної версії, високу вартість, складність налаштування, проблеми з синхронізацією та необхідність Інтернет-з'єднання для доступу до паролів.

RoboForm (рисунок 1.2) широко використовується серед бізнес-користувачів для управління паролями [22]. Він відзначається зручним дизайном, підтримує 2ФА та використовує шифрування AES-256 для захисту даних. RoboForm доступний на різних платформах і сумісний з основними браузерами. Основними функціями МП є генерація паролів, можливість

входу в один клік та безпечний обмін даними.

Переваги RoboForm включають можливість вибору між автономним або хмарним зберіганням, безпечні паролі та можливості спільного використання папок, моніторинг dark web для підвищення безпеки.

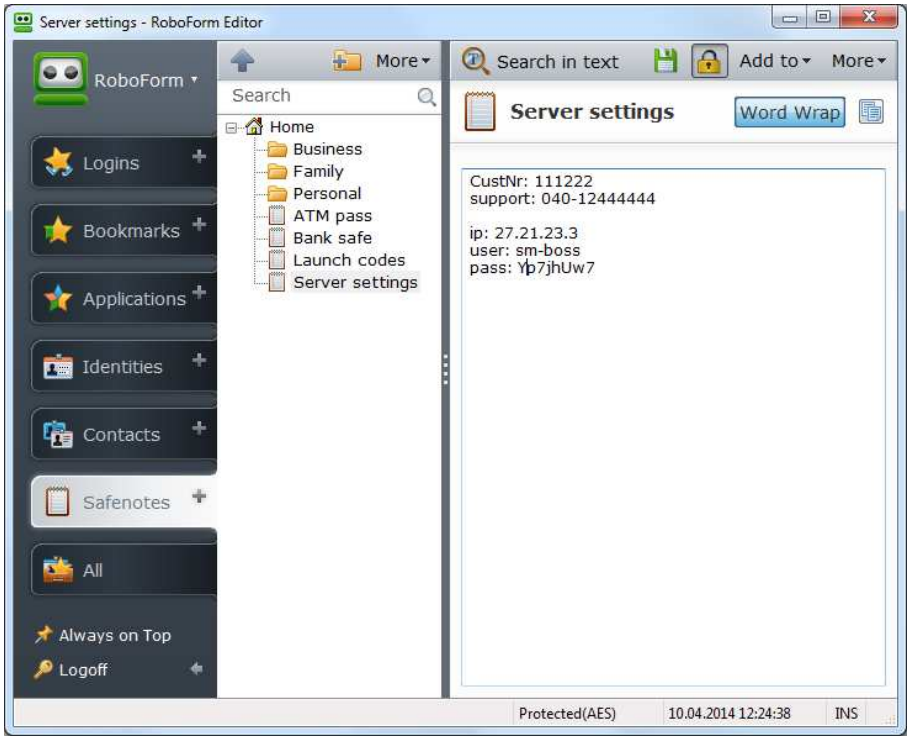


Рисунок 1.2 – RoboForm

До недоліків можна віднести обмежену функціональність безкоштовної версії МП, можливі проблеми з синхронізацією між різними пристроями. Хоча RoboForm підходить і для індивідуальних користувачів, його основні функції часто спрямовані на бізнес-клієнтів.

1Password вирізняється безлімітною кількістю одночасних підключень і простотою та зручністю використання (рисунок 1.3) [19]. Основою безпеки МП є використання майстер-паролю, також доступна біометрична автентифікація. Додатковий рівень безпеки забезпечується 2ФА з використанням одноразових паролів.

Даний МП доступний для широкого кола платформ, включаючи Chrome OS та командний рядок. 1Password має розширення для основних браузерів і можливість налаштування гостьових облікових записів для

спільного використання паролів. Унікальними функціями є Watchtower - сканер dark web, який попереджає користувачів про потенційні загрози, та режим подорожі для приховування конфіденційних даних.

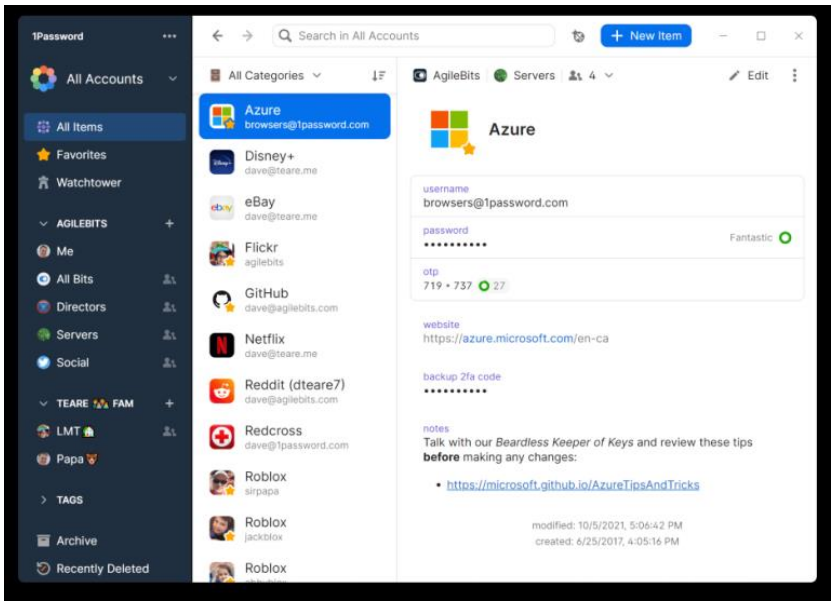


Рисунок 1.3 - 1Password

До переваг 1Password можна віднести перевірки щодо скомпрометованих паролів, підтримка користувачів електронною поштою, та привабливі моделі ціноутворення та перспектива функції ключів доступу.

Недоліки 1Password включають складність початкового налаштування, відсутність безкоштовної версії, можливі проблеми з синхронізацією між пристроями, а також те що інтерфейс програми може бути менш інтуїтивним енж у аналогів.

NordPass (рисунок 1.4) дозволяє забезпечити високий рівень онлайн-безпеки завдяки використанню шифрування XChaCha20 з подвоєною довжиною ключа та архітектуру нульового розкриття, що забезпечує надійний захист даних [22]. МП характеризується простотою використання та включає біометричний вхід, майстер-пароль та 2ФА. NordPass сумісний з основними платформами та браузерами. Він пропонує функції, такі як сканер витоку даних, автономний режим, зручну організацію даних і можливості оптичного розпізнавання символів.

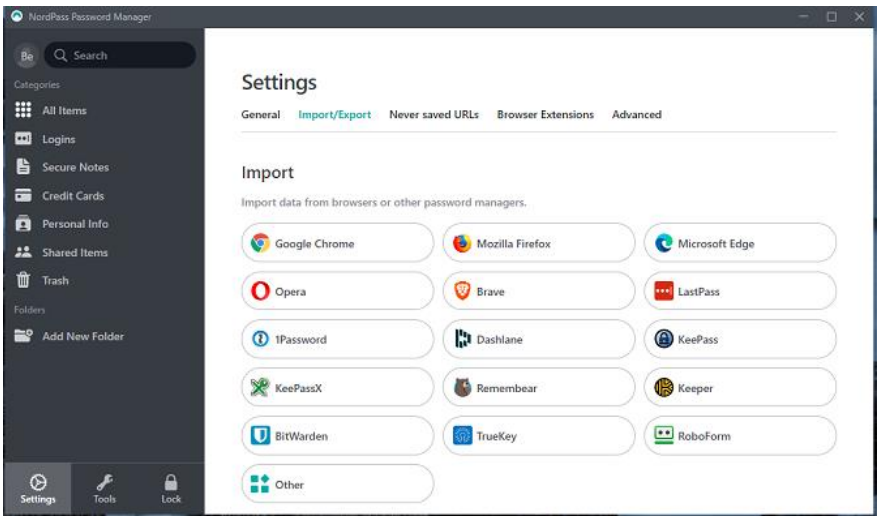


Рисунок 1.4 – NordPass

Перевагами NordPass є вдосконалена модель шифрування XChaCha20, багаторівневий процес автентифікації, підтримка ключів доступу та доступні економічні плани. Недоліками є обмежені функції у безкоштовній версії, незручний процес імпорту даних та синхронізації між пристроями, недостатня підтримка старих платформ, відсутність функції спільного досту

Zoho Vault [23] є універсальним рішенням для управління паролями, орієнтованим як на приватних осіб, так і на підприємства (рисунок 1.5). Інтеграційні можливості стоять на передньому плані: Він легко інтегрується з існуючими службами ідентифікацій, такими як AD/LDAP, Google Workspace, Microsoft Office 365, що спрощує імпорт паролів.

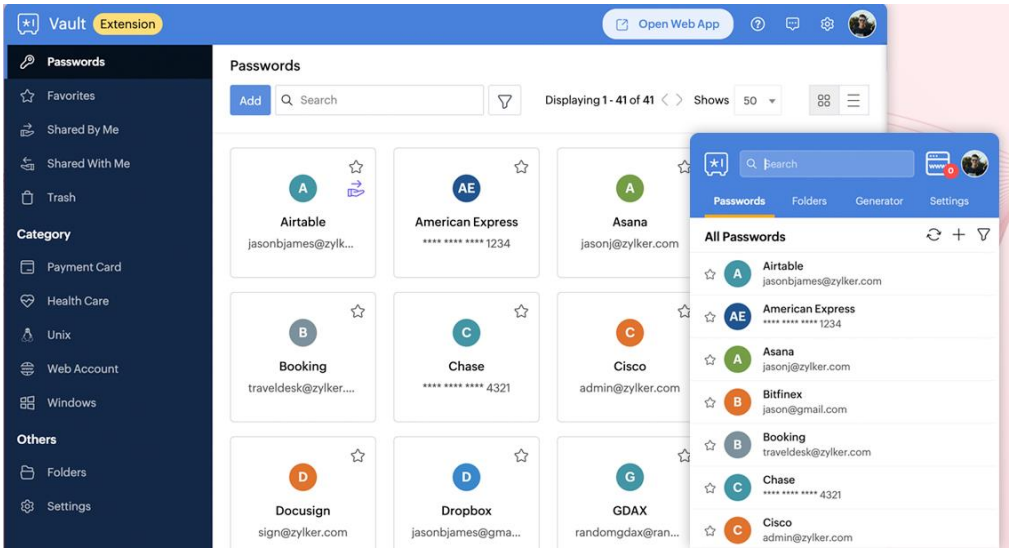


Рисунок 1.5 - Zoho Vault

Його розширення підтримують браузери Chrome, Firefox, Safari та інші, а мобільні додатки для Android та iOS роблять керування паролями зручним та підвищують доступність. Серед функції СКП можна виділити звіт про оцінку паролів, який вказує на слабкі або повторювані паролі, а також комплексні можливості аудиту. Zoho Vault забезпечує високий рівень безпеки, використовуючи архітектуру з нульовим розкриттям даних, яка гарантує, що навіть майстер-пароль не зберігається на серверах.

Переваги включають універсальне управління паролями для різних користувачів, безшовну інтеграцію з основними платформами, організований доступ до даних, функцію єдиного входу для хмарних додатків, автозаповнення та можливість використання VPN. Проте безкоштовна версія та мобільний додаток мають обмежені можливості, процес налаштування може бути складним, відсутність підтримки старих платформ створити труднощі у використанні цього інструменту.

Dashlane є преміум-менеджером паролів, відомим своїми можливостями обміну паролями та надійними функціями безпеки, такими як 2ФА та можливості біометричного доступу (рисунок 1.6) [18]. Серед його основних функцій – сканер Dark Web, вбудований VPN, перевірка та можливість безпечного обміну паролями, що робить його зручним для користувачів.

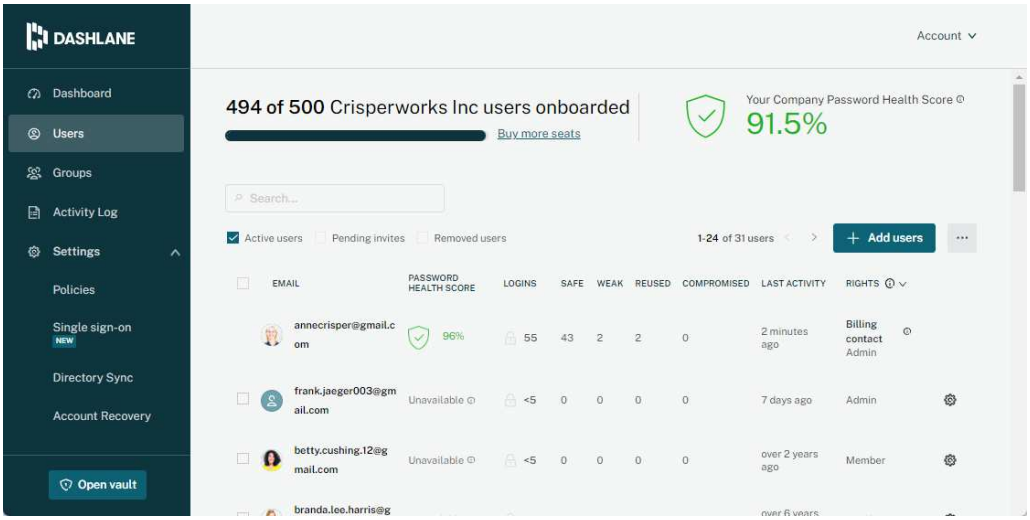


Рисунок 1.6 - Dashlane

Dashlane має інтуїтивно зрозумілий інтерфейс, що робить його легким у використанні. Комплексне сканування Dark Web дозволяє відслідковувати потенційні загрози, а вбудований VPN забезпечує шифрування трафіку. Ефективна перевірка паролів допомагає виявляти слабкі або зламані паролі, а безкоштовна версія дозволяє протестувати основні функції. Проте вартість підписки вища, ніж у конкурентів, а безкоштовна версія має обмежений функціонал. Деякі користувачі відзначають високі вимоги до ресурсів і можливі проблеми з синхронізацією між пристроями. Також відсутні деякі розширені функції, такі як імпорт паролів із телефонів

Passwarden від KeepSolid (рисунок 1.7) є комплексним рішенням, що забезпечує посилену онлайн-присутність для користувачів завдяки використанню шифрування AES-256-GCM, що гарантує гарантує захист даних від потенційних загроз [24]. СКП пропонує підтримку 2ФА та біометрії, що додатково підвищує рівень безпеки облікових записів.

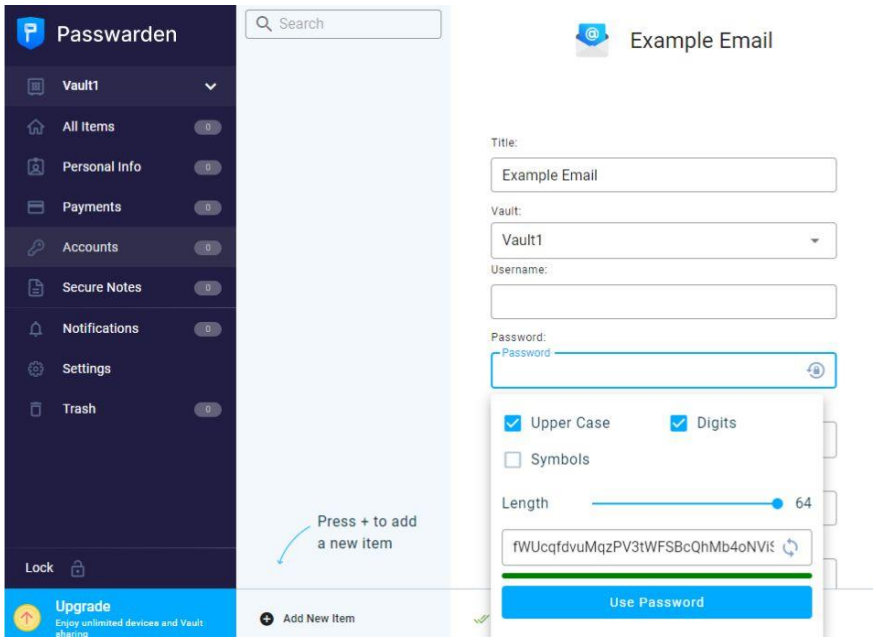


Рисунок 1.7 - Passwarden

Основні функції включають панель безпеки, що контролює працездатність паролів, режим додаткової безопеки для важливих даних, вбудований VPN для шифрування даних та забезпечення конфіденційності.

Passwarden характеризується високим рівнем захисту даних, інтуїтивно

зрозумілими додатками для різних платформ та можливістю безкоштовного використання основних функцій. Обмежені можливості інтеграції з іншими сервісами, труднощі з навігацією в інтерфейсі, відсутність розширених функцій та можливі затримки у відповіді служби підтримки обмежують використання МП.

Bitwarden (рисунок 1.8) це МП з відкритим вихідним кодом, який забезпечує зручність роботи для стаціонарних та мобільних користувачів, включаючи командний інтерфейс [25]. Основними функціями інструменту є розширена 2ФА та шифрування AES-256, що надійно захищає дані, ініціюючи шифрування головним паролем, який проходить через хешування перед зберіганням. Наскрізне шифрування гарантує, що дані залишаються захищемини навіть у випадку їх перехоплення. Функція екстреного доступу дозволяє довіреним особам отримати доступ до сховища в надзвичайних ситуаціях.

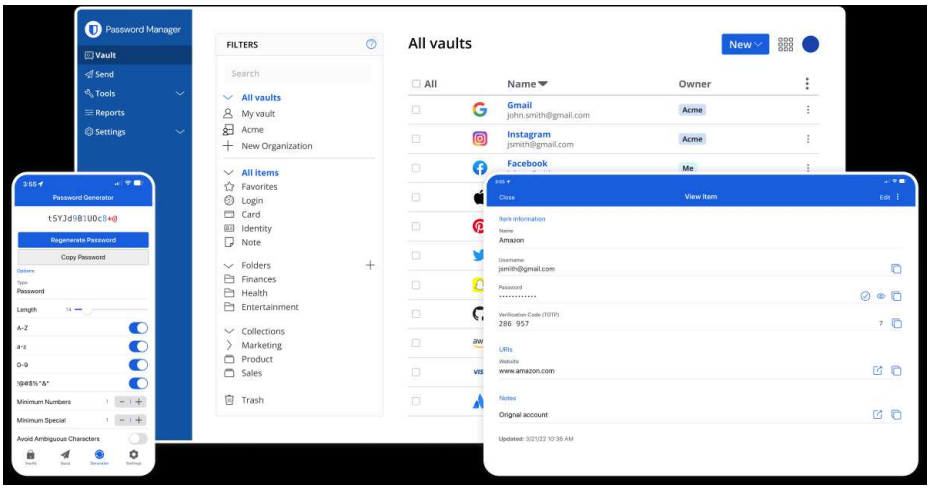


Рисунок 1.8 - Bitwarden

Додаткові функції включають можливість формування звіту про порушення безпеки та функціональності, генератор паролів та безпечний обмін даними.

Складний інтерфейс МП, обмежена безкоштовна версія та залежність від головного пароля, втрата якого може призвести до недоступності всіх даних, створюють певні ризики, які знижують надійність цього рішення для

зберігання та управління паролями.

Enpass (рисунок 1.9) пропонує спрощений і мінімалістичний підхід до управління паролями, орієнтуючись на автономне використання, але також забезпечує можливості міжплатформної синхронізації з використанням хмарних сервісів, таких як OneDrive, Dropbox і iCloud [26].

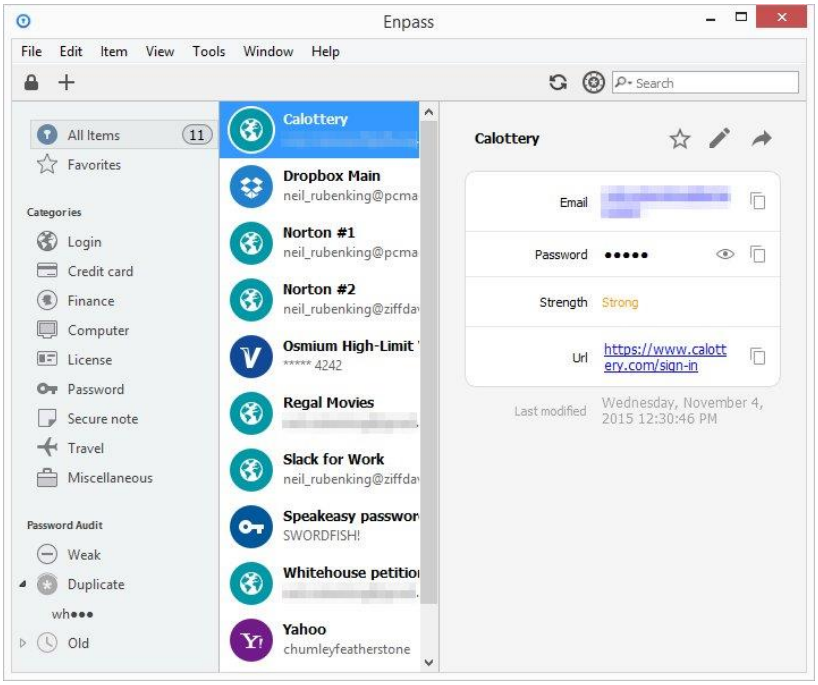


Рисунок 1.9 - Enpass

Основні функції інструменту забезпечують високий рівень безпеки даних шляхом шифрування AES-256 у поєднанні з SQLCipher. Використання додаткового файлу, що містить ключ шифрування та доповнює основний ключ, забезпечує оптимальний рівень захисту. МП дозволяє створювати надійні паролі, зберігати їх та відслідковувати їх безпеку завдяки функції моніторингу.

Enpass є відмінним вибором для користувачів, які шукають простий і безпечний менеджер паролів, орієнтуючись на автономне використання. Його функції шифрування та підтримка міжплатформової синхронізації роблять його надійним рішенням для зберігання паролів. Проте, слід також врахувати недоліки Enpass, зокрема обмежені можливості безкоштовної мобільної версії, складний інтерфейс та залежність від хмарних сервісів.

Зручним МП, що призначений для захисту особистих даних користувачів є Sticky Password [27]. Вбудований генератор паролів допомагає створювати складні паролі, які важко зламати, а функція автозаповнення спрощує процес входу в облікові записи (рисунок 1.10). Інструмент доступний на популярних платформах, таких як Windows, macOS, Android та iOS, а також надає розширення для багатьох браузерів.

Функції МП забезпечують створення паролів, шифрування даних AES-256 та можливості 2ФА та біометричної автентифікації, що відповідає сучасним вимогам безпеки.

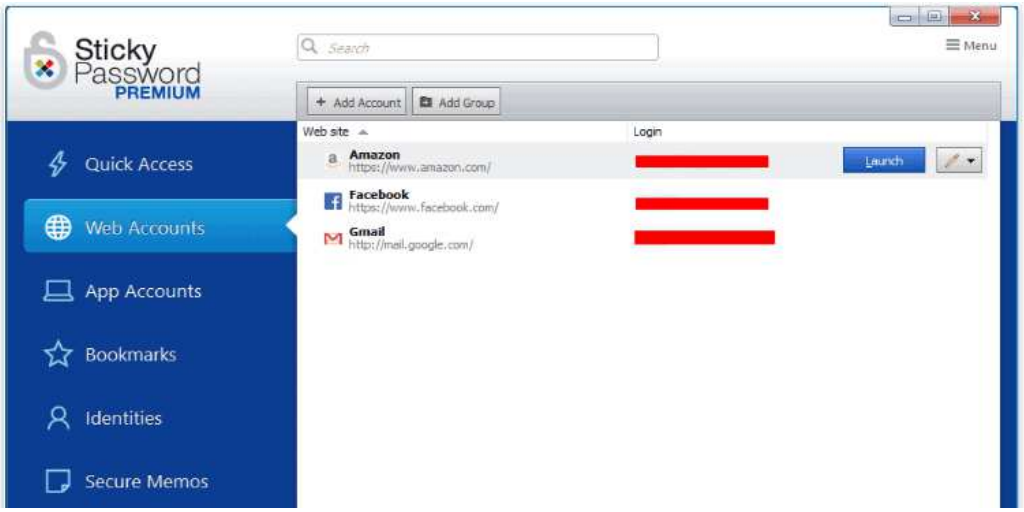


Рисунок 1.10 - Sticky Password

Sticky Password є надійним МП, що пропонує високий рівень захисту особистої інформації. Вбудований генератор паролів полегшує створення надійних паролів, а функція автозаповнення спрощує вхід в облікові записи. Користувачі можуть скористатися безкоштовною версією, яка дозволяє протестувати основні функції. Однак вона має обмеження, а деякі функції доступні лише в платній версії. Крім того, для оптимального використання МП може знадобитися час на налаштування. Втрата головного пароля також може призвести до втрати доступу до всіх даних, що є значним ризиком.

LastPass є надійним інструментом для управління паролями, що пропонує різноманітні функції, такі як багатофакторна автентифікація (БФА) і кросплатформна підтримка (рисунок 1.11) [28].

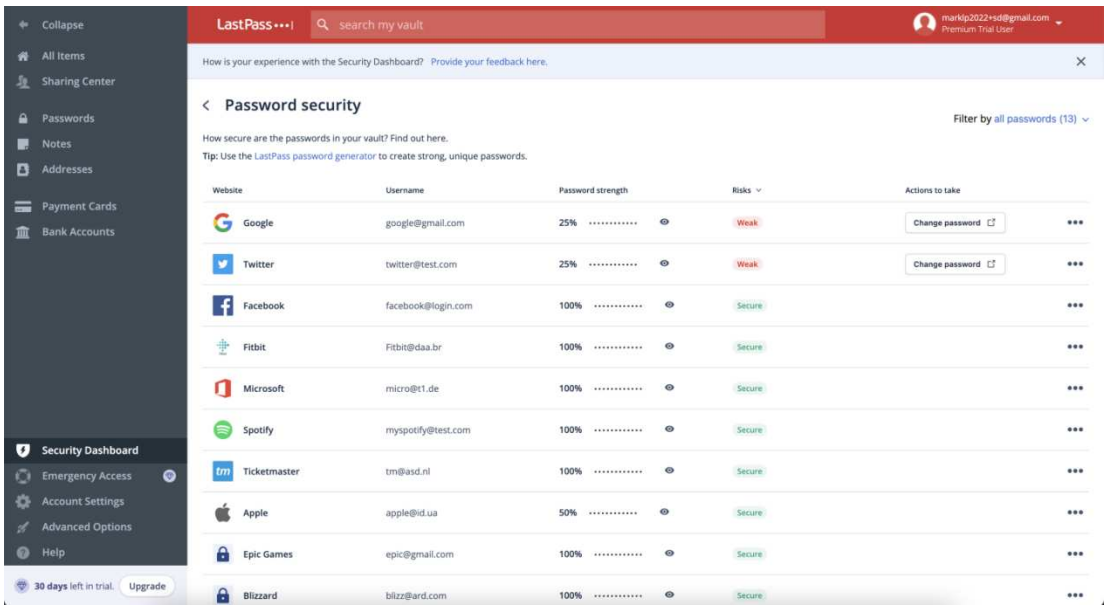


Рисунок 1.11 - LastPass

Його функції автозаповнення та автозбереження спрощують процес входу в облікові записи. Безкоштовна версія є функціональною, а значна кількість розширень для браузерів підвищує зручність використання МП. Проте, відсутність підтримки через чат або телефон можуть викликати затримки у відповіді, а проблеми з безпекою можуть бути суттєвими недоліками для деяких користувачів.

RememBear є зручним менеджером паролів, розробленим командою TunnelBear VPN (рисунок 1.12) [29]. Його зрозумілий інтерфейс зумовлює його вибір для спрощення процесу управління паролями. МП забезпечує безпечне зберігання даних завдяки шифруванню банківського рівня та дозволяє зберігати, синхронізувати та генерувати паролі. Додатково передбачена можливість зберігання нотаток та даних кредитних карток, що спрощує автозаповнення.Однією з його головних переваг є необмежене сховище та спрощена процедура відномлення майстер-паролю. можливість зберігати необмежену кількість паролів і даних. Процес імпорту паролів з інших менеджерів може бути небезпечним. Безкоштовна версія МП обмежує доступ до більшості функцій і не дозволяє створювати резервні копії паролів, що може створити проблеми для цілісності та доступності даних.

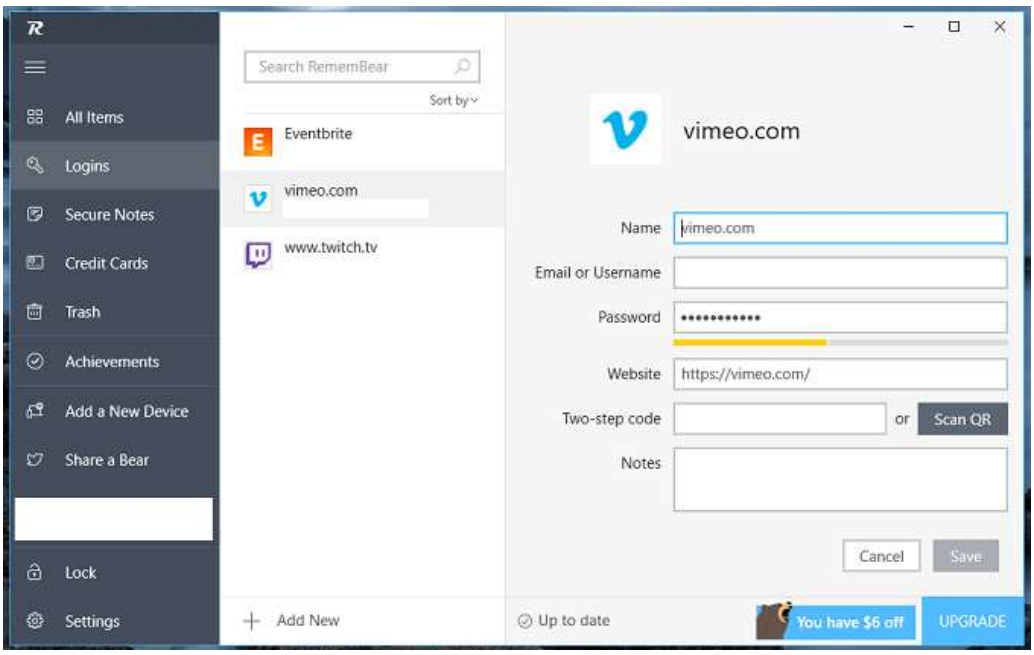


Рисунок 1.12 - RememBear

Passbolt (рисунок 1.13) МП з відкритим вихідним кодом, розроблений переважно для компаній та промислових підприємств [30]. Основні його характеристики включають можливість адаптації під специфіку виробництв, безпечний доступ за рахунок використання майстер-пароля разом із закритим ключем та прозорість для перевірки безпеки.

Відкритий вихідний код для самостійних модифікацій, безпечний обмін паролями між користувачами та безкоштовний доступ для індивідуальних користувачів є перевагами даного інструменту.

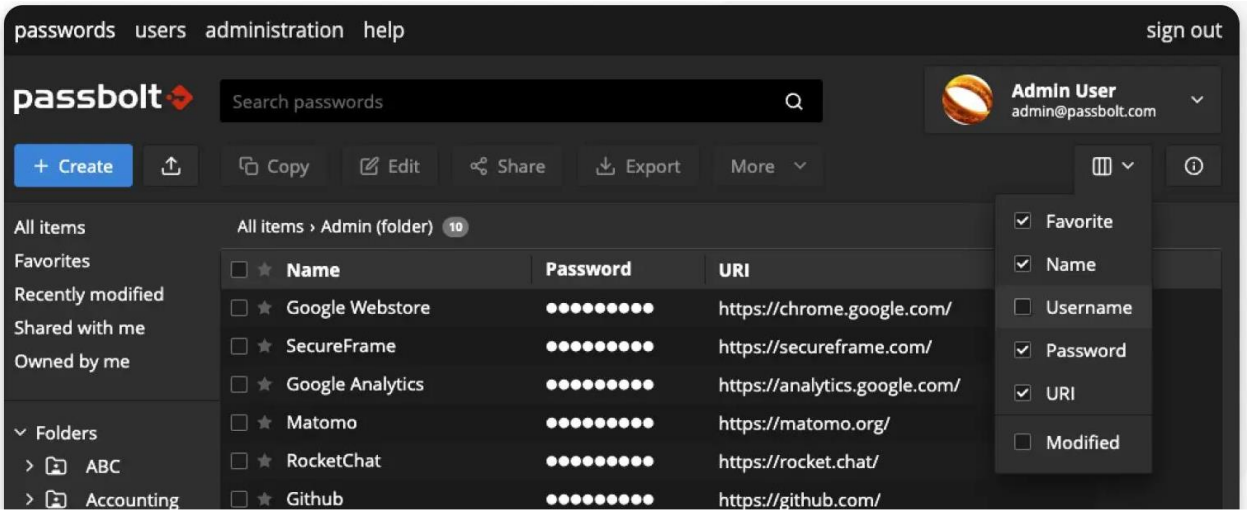


Рисунок 1.13 - Passbolt

Відсутність мобільних додатків, необхідність самостійного вирішення проблем може утруднювати практичне використання Passbolt. Хостинг-рішення може вимагати значних технічних знань. Незважаючи на безпеку, використання інших методів шифрування може не відповідати сучасним стандартам.

В таблиці 1.1 наведено порівняльні характеристики розглянутих МП.

Таблиця 1.1 – 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	Відсутнє	Chrome, Firefox, Safari, Edge, Brave, Vivaldi
RoboForm	Відсутнє	Chrome, Edge, Firefox, Opera
LastPass	1 GB	Chrome, Firefox, Safari, Opera, Edge, застаріла версія Edge
RememBear	Відсутнє	Chrome, Firefox и Safari
Zoho Vault	100 MB	Chrome, Firefox, Safari, Edge, Brave и Vivaldi
Passbolt	Відсутнє	Chrome, Firefox
Bitwarden	1 GB	Google Chrome, Firefox, Vivaldi, Opera, Microsoft Edge, Safari, Tor, Brave

Дослідження систем керування паролями дозволило визначити ключові аспекти, які суттєво впливають на безпеку та ефективність зберігання та обробки паролів на сучасних підприємствах.

1.3 Методи шифрування в системах керування паролями

СКП використовують різні методи шифрування для забезпечення захисту збережених паролів та особистої інформації [11-15, 31], зокрема:

- симетричне шифрування;
- асиметричне шифрування;
- хешування;
- криптографічні бібліотеки;
- двофакторна автентифікація.

AES (Advanced Encryption Standard) використовує один ключ для шифрування та дешифрування даних та забезпечує високий рівень безпеки і підтримує різні розміри ключів (128, 192, або 256 біт). AES вважається одним із найбільш безпечних симетричних алгоритмів шифрування і використовується в багатьох критичних системах. Порівняно з іншими методами (наприклад, RSA), AES є швидким в обчисленнях, особливо при великих обсягах даних. Підтримка різних розмірів ключів дозволяє налаштовувати рівень безпеки під конкретні вимоги.

Ситетричне шифрування вимагає безпечного обміну ключами. Якщо зловмисник отримає доступ до ключа, всі зашифровані дані можуть бути дешифровані.

RSA (Rivest–Shamir–Adleman) використовує пару ключів (публічний і приватний) для шифрування даних, що зменшує ризик компрометації даних під час передачі. Алгоритм є стійким до багатьох видів атак. Для забезпечення високого рівня безпеки потрібні дуже ключі великого розміру, наприклад 2048 біт і більше, що збільшує час і ресурси для обробки. Тому його часто використовують для шифрування ключів, а не для безпосереднього шифрування даних.

Алгоритми хешування bcrypt, Argon2, PBKDF2 не шифрують паролі, а перетворюють їх на незворотні хеші. Це означає, що навіть якщо хеш зламано, вихідний пароль не може бути відновлений. Дані алгоритми

розроблені для уповільнення процесу обчислення хешів, що робить атаки грубою силою менш ефективними. Хоча це перевага може негативно впливати на швидкість, якщо хешування потрібно виконувати дуже часто. Додавання унікальних даних «солі» (salt) до кожного пароля запобігає використанню заздалегідь обчислених таблиць хешів (rainbow tables). Якщо алгоритм не налаштований правильно (наприклад, використання недостатньо високого кількості ітерацій), його безпека може бути знижена.

Деякі СКП можуть використовувати менш поширені алгоритми шифрування, які реалізують власні методи захисту, наприклад шифрування на основі обчислювальних графів (Vigènere, etc.).

Безпека менеджерів доступу базується на використанні відомих криптографічних бібліотек, наприклад OpenSSL, libsodium та ін., що підтримують сучасні та найбільш надійні алгоритми шифрування, забезпечуючи сумісність із сучасними вимогами безпеки. Помилки або вразливості в бібліотеках можуть впливати на безпеку СКП, що їх використовує. Використання таких бібліотек вимагає глибоких знань у галузі криптографії для правильного налаштування.

Використання 2ФА, хоча і не є методом шифрування, але часто реалізується в МП для додаткового рівня захисту, що дозволяє зменшити ризик НД. Наприклад, у випадку, коли зловмисник отримав пароль, необхідне підтвердження доступу за допомогою другого фактору, одноразового коду або біометричних даних. Це знижує ризик компрометації облікових записів та фішингових атак. Деякі форми 2ФА зумовлюють необхідність додаткового обладнання або додатків, що може бути незручним. Залежність від зовнішніх факторів може спричинити проблеми з відновленням доступу.

Розглянуті методи шифрування та захисту використовується в СКП для забезпечення максимальної безпеки. Симетричні алгоритми пропонують швидке і надійне шифрування даних, але потребують безпечного зберігання ключів. Асиметричні - додають безпеку в передачі ключів, але працюють

повільніше. Хешування із сіллю забезпечує надійний захист паролів, особливо проти атак грубою силою. Однак кожен метод має свої слабкі сторони, і найбільш безпечні СКП використовують комбінацію цих методів для досягнення балансу між безпекою і продуктивністю.

1.4 Вимоги до безпечних інструментів керування паролями

СКП виконують важливу роль у забезпеченні безпеки доступу до ресурсів та облікових записів, тому вони повинні відповідати ряду вимог, зокрема:

- безпечного зберігання даних для запобігання витоку інформації;
- надійного шифрування для забезпечення конфіденційності та цілісності;
- захист від атак таких як фішинг або атаки через грубу силу;
- надійна автентифікація;
- аудит безпеки з метою перевірки системи на вразливості;
- зручність використання;
- надійність резервного копіювання та відновлення;
- підтримка відкритих стандартів для забезпечення прозорості та можливості інтеграції з іншими системами.

Система управління паролями повинна використовувати сучасні криптографічні алгоритми для шифрування. Дані повинні бути захищені як на стороні клієнта (локальне зберігання), так і під час передачі (якщо МП використовує хмарну синхронізацію). Майстер-пароль повинен бути надійно захищений і не зберігатися в явному вигляді.

СКП повинна включати механізми для запобігання спробам підбору пароля, наприклад обмеження кількості спроб входу або уповільнення процесу після кількох невдалих спроб. Додаткові механізми, такі як БФА або біометричні засоби, допомагають захистити дані від НД.

В СКП повинні бути реалізовані наступні функції:

- генерації складних паролів та їх надійного зберігання;
- автоматичного заповнення форми при вході у облікові записи;
- синхронізації даних між різними пристроями (комп'ютерами, смартфонами, планшетами) через захищені канали;
- резервного копіювання паролів з можливістю їх безпечного відновлення в разі втрати доступу до пристрою або даних;
- моніторингу облікових записів, що дозволяє виявити, чи потрапляли паролі до списків скомпрометованих даних, наприклад, через злами баз даних (БД).

У випадку використання хмарної синхронізації даних, усі паролі повинні бути зашифровані на пристрої користувача перед передачею на сервери, щоб уникнути можливості доступу до незашифрованих даних на стороні провайдера. Навіть розробники СКП чи власники хмарних серверів не повинні мати можливості отримати доступ до паролів користувачів.

Для підвищення рівня безпеки СКП необхідно регулярно оновлювати політику безпеки, щоб виправляти можливі вразливості та відповідати новим загрозам. Система повинна попереджати користувачів про слабкі, повторювані або давно незмінювані паролі та рекомендувати їх оновлення. Користувачі повинні мати можливість звертатися до служби підтримки для вирішення технічних проблем або отримання консультацій.

СКП має поєднувати високий рівень безпеки, зручність у використанні та надійний захист конфіденційних даних. Важливими функціями, що забезпечують їх ефективність у сучасному кіберсередовищі, є шифрування на стороні клієнта, двофакторна автентифікація, резервне копіювання та перевірка безпеки паролів.

2. ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ТА АЛГОРИТМІВ РОБОТИ СИСТЕМ УПРАВЛІННЯ ПАРОЛЯМИ

2.1 Керування паролями доступу до ресурсів підприємства

У своїй діяльності організації та підприємства використовують велику кількість додатків, вебсервісів і спеціалізованого програмного забезпеченя (ПЗ) [1-3]. Часто для ефективної роботи цим програмам необхідний доступ до інших додатків, серверів або БД. Процеси комунікації та доступу, як правило, автоматизуються за рахунок включення облікових даних до файлів конфігурації та скриптів. Однак зростання кількості облікових записів ускладнює адміністратору систем задачу ідентифікації, оновлення та керування ними. Це може призвести до того, що облікові дані залишаються незмінними протягом тривалого часу, що створює ризики НД до чутливої інформації [4-7].

Для вирішення цієї проблеми використовуються спеціалізовані СКП доступу до ресурсів підприємства (рисунок 2.1). Вони усувають необхідність зберігати конфіденційні дані у відкритому вигляді. Замість цього додатки можуть отримувати необхідні дані через запит до СКП запит за допомогою API [32].

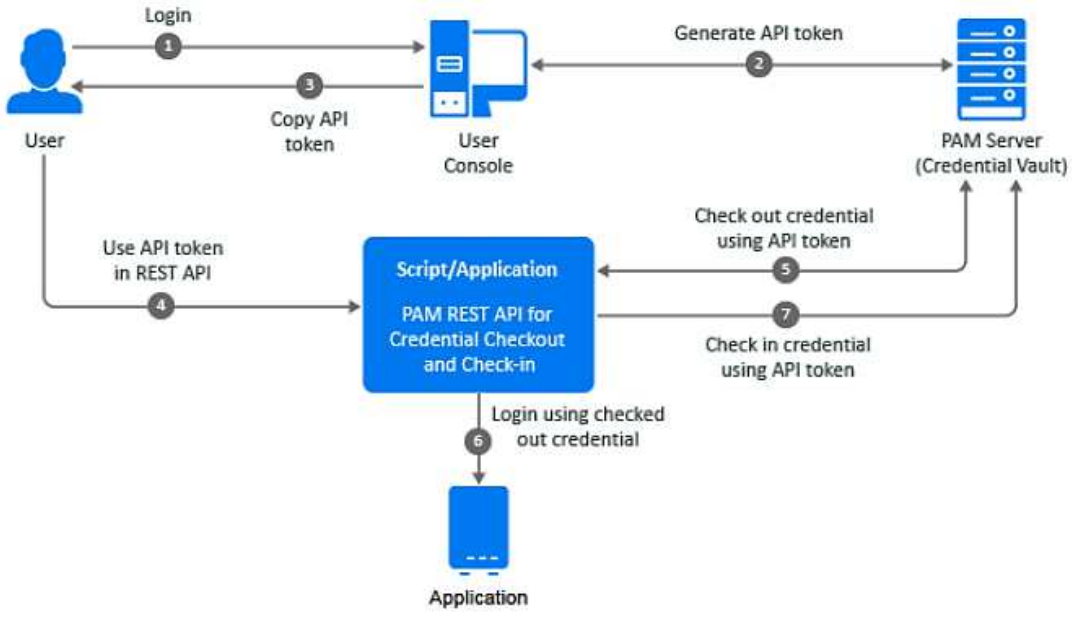


Рисунок 2.1 – Принцип роботи СКП

Такий підхід дозволяє захистити облікові дані, автоматично оновлювати паролі, а також призначати надійні й унікальні паролі без втручання адміністратора. Це підвищує загальний рівень безпеки та зменшує ризики компрометації даних.

СКП є основним інструментом для захисту облікових записів, що забезпечують доступ до важливих корпоративних систем, БД і сервісів. Проведені дослідження дозволяють визначити, що для ефективного функціонування СКП необхідно реалізувати наступні функції:

- генерації ключів;
- шифрування паролів;
- зберігання паролів;
- автентифікація користувачів;
- безпечний обмін даними;
- оновлення паролів і ключів.

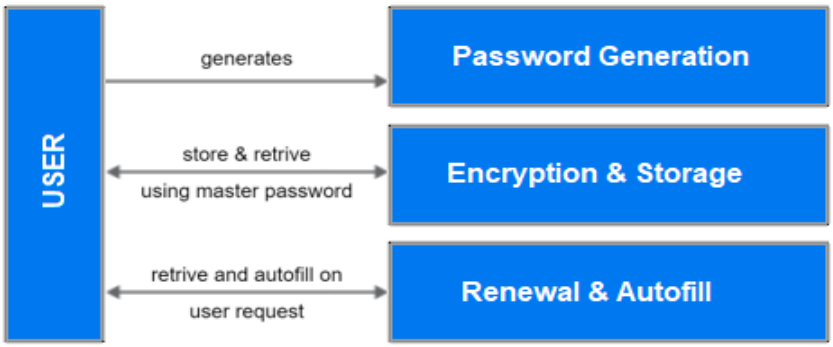


Рисунок 2.2 – Функції СКП

Використання криптографічних методів, таких як шифрування, хешування та додавання солі, є важливим елементом забезпечення конфіденційності, цілісності й безпеки облікових даних. Хешування є одним із основних методів захисту паролів у сучасних системах керування доступом. Це однонаправлений процес, перевага якого полягає в тому, що паролі не зберігаються у відкритому вигляді і їх розкриття практично неможливе. Використання «солі» дозволяє підвищити захист паролів від атак за допомогою попередньо обчислених таблиць хешів, а також значно

ускладнює перебір паролів. Завдяки додаванню «солі» навіть однакові паролі отримують різні хеші. Найбільш ефективним методів захисту даних, особливо при їх зберіганні, є шифрування. В СКП воно забезпечує перетворення пароля у вигляд, який неможливо прочитати без наявності приватного ключа. Цей процес дозволяє захистити облікові дані від НД навіть у разі компрометації БД або витоку інформації.

2.2 Алгоритми роботи менеджера паролів

Використання криптографічних хеш-функцій, таких як SHA-256, залишається поширеним підходом для зберігання паролів. Однак ці методи можуть бути вразливими до атак попереднього обчислення (lookup table, rainbow table) [8-10, 31-35]. Для захисту від таких атак у більшості сучасних СКП додатково використовують випадкову «сіль», що робить кожен хеш унікальним та підвищує стійкість до атак. Проте навіть при її використанні можливі атаки з використанням словників (dictionary attacks). Відповідно, деякі СКП впроваджється техніка ключового розтягування (key stretching), яка збільшує час обчислення кожного хешу, роблячи атаки на паролі менш практичними. Рішення, які комбінують хешування з асиметричним шифруванням, демонструють значний потенціал у підвищенні безпеки паролів та забезпечують захист від атак із використанням попередньо обчислених таблиць та захищають паролі від крадіжок.

У спеціалізованих СКП важливо враховувати комплексний підхід до захисту. Використання БФА, надійних алгоритмів шифрування та управління ключами допомагає мінімізувати ризики. СКП можуть бути інтегровані з іншими системами для підвищення рівня захисту корпоративних даних.

2.2.1 Алгоритм зберігання та управління обліковими даними

Для реалізації СКП необхідно розглянути алгоритми, які забезпечать надійне зберігання та управління обліковими даними.

Для реалізпції процесу генерації ключів необхідно:

- здійснити збір інформації про систему, $Info_H$ – дані про пристрій, наприклад, ідентифікатор процесора, відеокарти, обсяг оперативної пам'яті, серійні номери накопичувачів тощо;
- використати функцію SHA-512 для обчислення Key_H, що є ключем, який згенерований на основі даних про пристрій. Його можна обчислитивати наступним чином:

$$Key_H = SHA512(Info_H).$$

- використати контрольну суму файлів прогрми для Key_S - інформації про поточну версію клієнтського ПЗ, наприклад, контрольної суми файлів програми, із застосуванням алгоритму MD5 або SHA-256.

Шифрування паролів передбачає, що:

- при зберіганні паролів використовується симетричне шифрування за допомогою AES -256.
- унікальна «сіль» генерується для кожного пароля;
- шифрування паролів відбувається з комбінуванням Key_H та Key_S:

$$Password_E = AES - Encrypt(Password + Salt, Key_H + Key_S)$$

Для реалізації процесу зберігання паролів необхідним є:

- використання захищеного сховища, наприклад, БД, зашифрованих файлів, для зберігання зашифрованих паролів і солі.
- зберігання інформації про «сіль» поряд із зашифрованими паролями.

У процесі автентифікації необхідним є:

- запит для введення майстер-пароля під час входу користувача;
- використання Key_H та Key_S для дешифрування збережених паролів з метою перевірки автентифікації;
- процедура надання доступу до сховища паролів при успішному розшифруванні та збігу із введеним паролем.

Обовязковим умовами для реалізації безпечного обміну паролями є:

– використання захищених каналів зв’язку, зокрема HTTPS;

– шифрування даних перед відправленням, використовуючи унікальний ключ для кожної сесії, наприклад з використанням одноразових ключів або тимчасових токенів [35].

Забезпечення можливості оновлення паролів і ключів включає:

– можливість користувачів оновлювати дані та генерувати нові ключі в разі їх компроментації, втраті або пошкодженні;

– при оновленні пароля обов’язковий перерахунок «солі» та шифрування нового паролю, використовуючи оновлені ключі.

Реалізація даних функцій забезпечить основу для побудови надійної СКП. Важливо також враховувати додаткові аспекти безпеки, такі як регулярні оновлення ПЗ, використання БФА та захист від атак за допомогою шкідливого ПЗ.

2.2.2 Алгоритми реєстрації та автентифікації користувача

Алгоритми реєстрації та автентифікації користувача, який можна використовувати для реалізації СКП включає наступні кроки:

1. Реєстрація нового користувача (пристрою):

– на сервер надсилається згенерований Key_H пристрою або пароль користувапча;

– сервер генерує випадкову 512-бітову послідовність – $Salt_{reg}$, що можна реалізувати за допомогою використання криптографічно стійкого генератора випадкових чисел;

– обчислення на стороні сервера $Key_{\text{Т}}$ таким чином:

$$Key_{\text{Т}} = SHA512\big(Key_H \,\big|Salt_{reg}\big).$$

Після чого $Key_{\text{Т}}$ зберігається в БД 2ФА.

– сервер повертає клієнту $Key_{\text{Т}}$ – ключ, що буде використовуватися для генерації одноразових кодів при вході в систему, який необхідно зберегти в надійному місці.

2. Автентифікація існуючого користувача (пристрою):

- користувач вводить тимчасовий одноразовий пароль (ТОП), який надсилається на сервер разом із Key_H;
- сервер шукає в БД відповідний Key_H і порівнює ТОП для Key_{T} з тим, що був надісланий клієнтом, включаючи перевірку коректності ТОП на основі тимчасового вікна, зазвичай 30 секунд.
- у разі збігу одноразових кодів сервер повертає клієнту два JSON Web Tokens (JWT-токени): один - для виконання дій з паролями, наприклад, створення, оновлення, видалення, другий - для повторної автентифікації по закінченню часу дії першого токена, що дозволяє не вводити код кожного разу, а підтримувати сесію активною протягом певного часу.

Такий підхід дозволяє не використовувати майстер-пароль для автентифікації, що може підвищити зручність використання та знизити ризики, пов'язані з його втратою. Використання ТОП забезпечує високий рівень безпеки завдяки 2ФА. Це дозволяє запобігти НД до облікового запису, навіть якщо зловмисник отримує доступ до Key_H. JWT використовуються для спрощення управління сесіями та автентифікацією. Вони дозволяють передавати інформацію між сервером і клієнтом та можуть бути перевірені без необхідності звернення до БД.

Заходи для підвищення безпеки розглянуторго алгоритму включають:

- зберігання Key_{T} у зашифрованому вигляді для захисту від НД;
- регулярну ротацію ключів Key_{T} та $Salt_{reg}$ для підвищення безпеки;
- реалізацію механізмів захисту від атак повторного використання та Brute Force, наприклад, шляхом блокування облікового запису після кількох невдалих спроб введення ТОП.

2.2.3 Алгоритм створення та редагування пароля

Алгоритм створення або редагування пароля на сервері включає кілька кроків для забезпечення високого рівня безпеки. Їх реалізація включає:

1. Перевірку валідності токена - сервер перевіряє дійсність токена для всіх вхідних запитів у блоці.

2. Отримання інформації про сервіс - клієнт надсилає серверу інформацію про сервіс, для якого потрібно отримати пароль.

3. Отримання «солі» - сервер повертає «сіль»для цього сервісу, псевдовипадкове n-бітне значення, яке генерується під час реєстрації сервісу.

4. Обчислення ідентифікатора пароля - клієнт обчислює ідентифікатор пароля ID_{pass} наступним чином:

$$ID_{pass} = SHA512(salt \mid login \mid Key_H)$$

де $login$ - логін користувача на сервісі.

5. Генерацію модуля для RSA2048 - клієнт генерує модуль для алгоритму RSA2048 на основі ідентифікатора пароля:

$$num = PBKDF2\left(SHA512,\ Id_{pass}[1:448],\ Id_{pass}[449:512],\ 200, 1024\right) mod(p \cdot q),$$

де p та q - це два простих числа, які разом формують модуль.

6. Обчислення значення на основі якого генерується відкрита експонента *e*:

$$Hash_e = SHA512(login \mid Info_H \mid Key_S).$$

Відкрита експонента *e* обчислюється:

$$e = PBKDF2\ (SHA512,\ \ Hashe\ [1:448],\ \ Hashe\ [449:512],\ 2000,\ \ 2048) mod\ (p \cdot q).$$

Якщо найбільший спільний дільник (НСД) $(e, (p-1) * (q-1)) \neq 1$, генеруються наступні 2048 біт до тих пір, поки НСД не стане рівним 1.

7. Шифрування пароля, шляом обчислення:

$$Pass_{Enc} = Password\ mod\ (p \cdot q).$$

8. Обчислення додаткової відкритої основи E_{totp} ($totp$ зберігається у зашифрованому вигляді у токені):

Спочатку обчислюється:

$$Hash_{totp} = SHA512(totp \mid Id_{pass}).$$

Після чого обчислюється E_{totp}, аналогічно з обчисленням відкритої основи, яку знає лише клієнт.

9. Відправки даних на сервер:

Клієнт надсилає серверу набір даних:

$$Id_{pass}, {Pass_{Enc}}^{E_{\text{totp}}}\ mod\ (p\ \cdot\ q), Key_S).$$

10. Обробки даних на сервері:

Сервер отримує набір даних та обчислює D_{totp} так, що:

$$E_{\text{totp}} \cdot\ D_{\text{totp}} =\ 1\ mod\big((p-1)\ (q-1)\big).$$

Сервер обчислює зашифрований пароль:

$$Pass_{Enc}\ =\ ({Pass_{Enc}}^{E_{\text{totp}}})^{D_{\text{totp}}}\ mod\ (p\ \cdot\ q).$$

11. Збереження даних у БД:

$$\big(Id_{pass}, Pass_{Enc}, Key_S\big).$$

Додаткове шифрування паролів із використанням RSA забезпечує захист від атаки «людина посередині» (MITM), якщо зловмисник отримує доступ до інформації про апаратне забезпечення. Затримка у генерації ключів через PBKDF2 може вплинути на тривалість виконання алгоритму, під час етапів створення або отримання пароля. Генерація чисел p і q може також вимагати первних часових витрат тому можна розглянути можливість кешування вже згенерованих значень для підвищення швидкості виконання.

Для підвищення ефективності алгоритму необхідно використати такі заходи як:

- оптимізація, зокрема варіанти реалізації, які дозволяють зменшити затримки під час генерації ключів;
- кешування - зберігання раніше згенерованих паролів або ідентифікаторів для зменшення тривалості генерації;
- моніторинг безпеки - регулярна перевірка алгоритму для виявлення вразливостей.

2.2.4 Алгоритм отримання пароля з сервера

Алгоритм отримання пароля з сервера складається з кількох етапів, які повторюють логіку, що використовується для створення або редагування пароля, зокрема:

1. Надсилання запиту на сервер із зазначенням ідентифікатора пароля користувача Id_{pass}.

2. Перевірку існування запису з вказаним ідентифікатором пароля в БД. Якщо такий запис не знайдено, сервер повертає статус Not Found. В іншому випадку переходить до наступного кроку.

3. Генерацію ключа для додаткового шифрування:

Сервер генерує ключ для додаткового шифрування за допомогою RSA, який обчислюється аналогічно до попереднього алгоритму. Відкрита експонента обчислюється наступним чином:

$$Hash_{totp} = SHA512(totp \mid Id_{pass}).$$

Далі сервер обчислює відкриту експоненту за допомогою PBKDF2, аналогічно попереднього алгоритму.

4. Відправку даних клієнту:

$$\left(Pass_{Enc}{}^{E_{\text{totp}}} \; mod \; (p \cdot q), Key_S\right),$$

де Key_S - інформація про версію ПЗ, з якою був створений пароль. Це вказує клієнту на необхідність оновлення пароля в БД, якщо він був створений за допомогою більш ранньої версії ПЗ.

5. Обробку даних клієнтом:

Обчислення відкритої основи E_{totp} (значення $totp$ зберігається в оперативній пам'яті після успішної автентифікації на сервері).

Далі клієнт обчислює закриту основу *d*:

$$\left(E_{\text{totp}} \cdot e\right) \cdot d = 1 \; mod \left((p-1)(q-1)\right).$$

6. Обчислення пароля шляхом піднесення до степеня *d* отримане, двічі зашифроване, значення:

$$password = (Pass_{Enc}{}^{E_{\text{totp}}})^{d} \equiv password^{\,e \cdot E_{\text{totp}} \cdot d}$$
$$\equiv password \bmod (p \cdot q).$$

7. Оновлення пароля:

Якщо пароль був створений більш ранньою версією ПЗ, передбачена можливість оновлення паролю клієнта на сервері.

Алгоритм забезпечує безпеку завдяки використанню RSA та додаткових рівнів шифрування, що мінімізує ризики перехоплення паролів. Інформація про версію ПЗ дозволяє клієнту бути впевненим у тому, що він використовує актуальні методи шифрування. Етапи, пов'язані з обчисленням закритої експоненти та шифруванням, можуть бути ресурсомісткими, що може вимагати оптимізації часу виконання.

З метою підвищення безпеки алгоритму можна використати наступні заходи:

- моніторинг за продуктивністю сервера під час виконання запитів на отримання паролів, особливо в пікові моменти навантаження;
- аудит безпеки для виявлення потенційних вразливостей у алгоритмі отримання та зберігання паролів;
- оновлення ПЗ та інформування користувачів про необхідність оновлення їх паролів, особливо якщо вони використовували застарілі версії.

2.3 Вразливості в системах керування паролями

Проблема безпеки паролів викликає багато суперечок у світі цифрових технологій. Проте, безумовно, важлимо мати унікальні паролі для різних облікових записів, адже це є одним із основних способів захисту особистої інформації. Хоча МП пропонують зручний спосіб зберігання та керування паролями, їх використання пов'язане з певними ризиками [15, 31, 33-36].

СКП часто стикаються з проблемами при спробі інтеграції з іншими програмами або синхронізації даних через ненадійні канали. Більшість онлайн-сервіси для управління паролями використовують скрипти, які

можуть бути вразливими до ін'єкцій на шкідливих веб-сайтах. Це створює ризики, оскільки користувачі можуть взаємодіяти з небезпечними елементами, не усвідомлюючи цього.

Аналіз вразливостей в інтерфейсах та взаємодіях дозволяє виявити потенційні загрози. Різні елементи інтерфейсу, такі як chrome і контент, можуть бути піддані атакам. Багато СКП не розділяють ці компоненти належним чином, що ускладнює виявлення зловмисних дій. Неправильна обробка кадрів може призвести до того, що зловмисники змусять користувача взаємодіяти з елементами інтерфейсу, які не є тим, з чим він передбачав працювати. Помилки в реалізації обміну даними можуть створити критичні вразливості, особливо якщо скрипти не можуть надійно ідентифікувати джерела запитів. Розширення, які використовуються онлайн-менеджерами паролів, можуть знижувати ефективність пісочниць у браузерах, створюючи небезпечні компроміси у безпеці. Це може дозволити зловмисникам обходити певні заходи безпеки.

Дослідження надійності захисту конфіденційної інформації, що забезпечується СКП, проводилося консалтинговою компанією з питань безпеки Independent Security Evaluators (ISE). У рамках проведеного аудиту безпеки було проаналізовано п'ять популярних МП, призначених для роботи з ОС Windows 10. У звіті [36], представлено аналіз безпеки таких МП, як 1Password (версії 4 та 7), Dashlane, KeePass та LastPass, а також висвітлено потенційні проблеми безпеки, виявлені під час дослідження (рисунок 2.3).

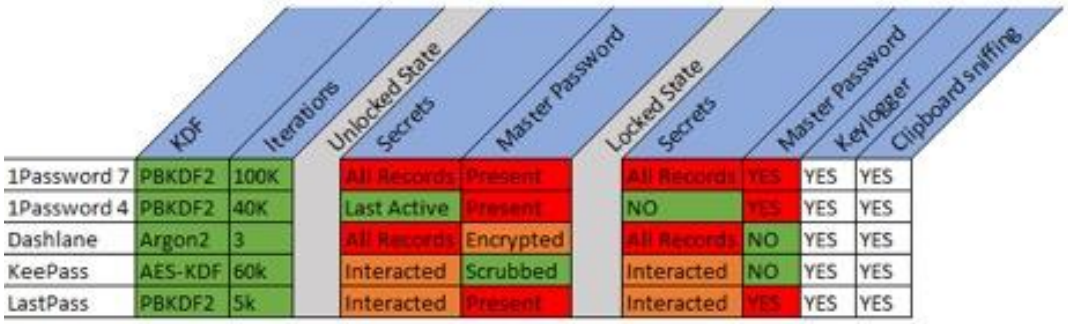


Рисунок 2.3 – Результати тестування безпеки МП

В результаті було виділено три стани функціонування СКП: «не запущено», «розблоковано» та «заблоковано». Основним висновком перевірки стало те, що всі МП продемонстрували ефективний захист даних у «не запущеному» стані, підтверджуючи їх здатність зберігати конфіденційну інформацію у безпечному режимі. Стан «не запущений» відповідає сценаріям використання, коли встановлений менеджер паролів не був активований або був закритий користувачем після його запуску. Стан «заблокований» характеризується ситуаціями, коли майстер-пароль не був введений, або менеджер паролів був заблокований вручну користувачем або автоматично.

У МП можуть виникати потенційні витоки даних у розблокованому та заблокованому станах за певних умов. У цих станах в 1Password і LastPass можливе перехоплення майстер-пароля, у Dashlane – витік усіх збережених записів, а в KeePass – отримання паролів та іншої конфіденційної інформації користувача. Також всі перевірені МП виявлялися вразливими до атак кейлоггерів і атак прослуховування буфера обміну [36]. Проте в стані «розблоковано» виявлено кілька вразливостей, що можуть бути використані зловмисниками для доступу до чутливої інформації. Наприклад, вразливості, пов'язані з кешуванням даних або недостатнім захистом в момент роботи програми, можуть створити можливості для атаки. У стані «заблоковано», МП показали хорошу захищеність, але в деяких випадках виявилися вразливими до атак, які експлуатують недоліки в механізмах блокування.

Основними проблемами використання СКП є:

− вразливість в управлінні пам’яттю, оскільки деякі МП не очищають чутливу інформацію з пам’яті належним чином після використання;

− недостатній захист при активному використанні, якщо МПзалишається активним, а комп'ютер залишається без нагляду, це може створити ризик НД;

− вразливості механізмів шифрування, хоча використовуються стійкі алгоритми шифрування, деякі реалізації СКП можуть мати недоліки,

які використовуються для зламу;

- ілюзію безпеки, оскільки маркетингові твердження компаній про те, що тільки користувач має доступ до паролів, можуть виявитися оманливими і в разі компрометації мережі розробника зловмисники можуть отримати доступ до збережених паролів..

Таким чином, хоча проаналізовані системи управління обліковими даниим забезпечують базовий рівень захисту, необхідно звертати увагу на налаштування безпеки та з періодичністю оновлювати ПЗ для підвищення безпеки конфіденційної інформації.

3. РОЗРОБКА СПЕЦІАЛІЗОВАНОЇ СИСТЕМИ КЕРУВАННЯ ПАРОЛЯМИ

3.1 Структура системи керування паролями підприємства

Схема структури СКП доступу до ресурсів підприємства включає основні компоненти, їх функції та взаємозв'язки між ними (рисунок 3.1).

Взаємодія між компонентами реалізована за допомогою:

– клієнтського інтерфейсу, що взаємодіє із серверною частиною через API, передаючи запити на реєстрацію, вхід та оновлення паролів;

– серверна частина взаємодіє з БД для збереження та отримання інформації про користувачів;

– механізми безпеки забезпечують захист даних на всіх етапах обробки інформації.

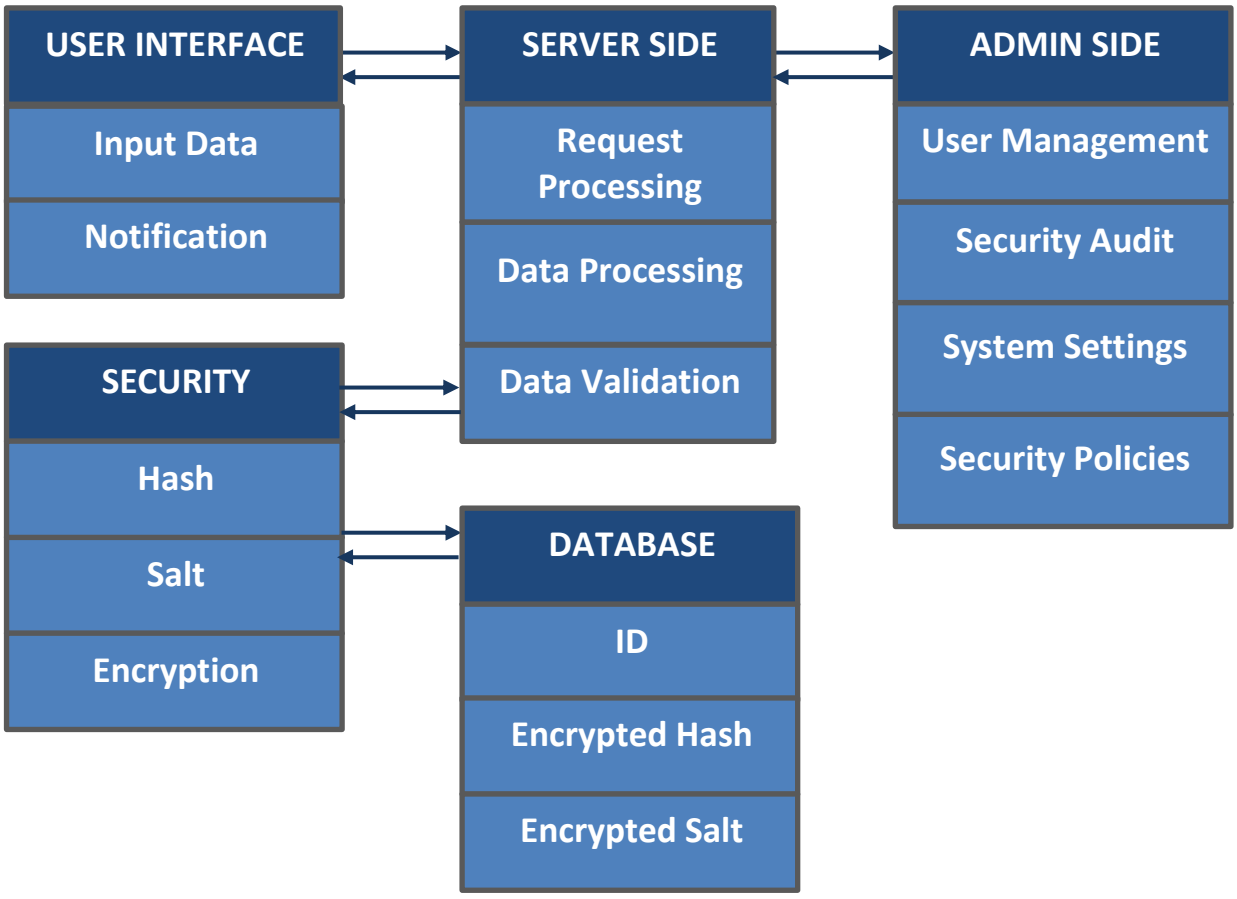


Рисунок 3.1 – Структура СКП

Клієнтський інтерфейс складається з наступних компонентів:

1. Форма реєстрації:

- поля для введення імені користувача та пароля;
- кнопка для підтвердження реєстрації.

2. Форма входу:

- поля для введення даних;
- кнопка для входу.

3. Сторінка оновлення даних:

- поля для введення старого пароля, нового пароля та підтвердження нового пароля;
- кнопка підтвердження виконання процедури оновлення пароля.

4. Сповіщення, зокрема повідомлення про успішні та невдалі дії при реєстрації, автентифікації, оновленні даних тощо.

Серверна частина забезпечує:

- обробку запитів - компоненти, що приймають запити від клієнтського інтерфейсу;
- валідацію даних - перевірка коректності введених даних, зокрема формат пароля, існування користувача тощо;
- управління користувачами - реєстрацію користувачів, оновлення даних про користувачів та їх видалення при необхідності.

База даних СКП включає збережену інформацію про користувачів, зокрема унікальний ID, що відповідає імені користувача, зашищений хеш пароля, «сіль» для хешування, а ткож може містити іншу інформацію, наприклад дату створення/оновлення запису.

Механізми керування даними реалізують обробку запитів на отримання, оновлення та видалення інформації.

Механізм безпеки включають:

- хешування паролів з використанням надійного криптографічного хеш-алгоритму;
- шифрування даних за допомогою асиметричного шифрування

для захисту хешів.

В поектованій СКП перебдачено можливість аудиту та ведення журналів таких як запис дій користувачів (успішні/неуспішні спроби входу, реєстрації), моніторингу системи на предмет аномалій та зловживань та ін.

Інтерфейс аднініструтора системи включає:

- управління користувачами;
- перегляд списку користувачів;
- можливість активації /видалення облікових записів;
- зберігання звітів та журналів активності.

Налаштування проектованої системи забезпечує налаштування політик безпеки, наприклад довжину пароля, частоту зміни пароля та ін, а ткаож конфігурацію методів автентифікації, наприклад застосування 2ФА.

Структура СКП доступу до ресурсів підприємства є надійною, орієнтованою на безпеку й зручність використання. Вона дозволячє забезпечити безпечну автентифікацію та контроль доступу, що дозволяє знизити ризик витоку чутливої інформації та забезпечити конфіденційність даних.

3.2 Алгоритм роботи проектованої системи

Для реалізації перелічених функцій розроблено алгоритми роботи проектованої СКП, що включає кілька основних етапів, зокрема: реєстрацію нових користувачів; процес автентифікації; оновлення даних.

На початку роботи СКП відбувається процес ініціалізаціі системи, зокрема завантаження бібліотек для хешування і шифрування, а ткож ініціалізація БД або файлу для збереження даних користувачів, імена, сіль, зашифровані паролі. На даному етапі відбувається перевірка ключів RSA або їх генерація за необхідності. Ініціалізація включає наступні кроки:

- запуск сервера, який обробляє запити від клієнтів через різні маршрути (наприклад, реєстрація, автентифікація, оновлення пароля);

- перевірка наявності ключів RSA для шифрування. Якщо файл з ключами доступний, відбувається його завантаження. Якщо ключі не знайдені в системі або файл пошкоджений, передбачена можливість генераціїї нової пари ключів RSA(рисунок 3.2).

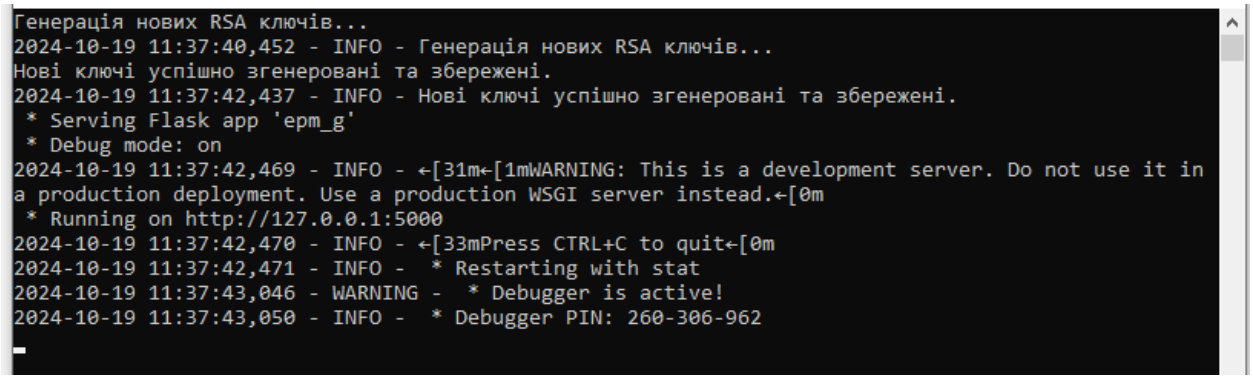


Рисунок 3.2 – Ініціалізація системи

Ключі зберігаються в файлах private_key.pem (рисунок 3.3) та public_key.pem (рисунок 3.4). Приватний ключ зберігається у захищеному місці для шифрування даних, публічний - для перевірки та автентифікації. Якщо ключі відсурні, а генерація нових не відбулася СКП припиняє роботу.

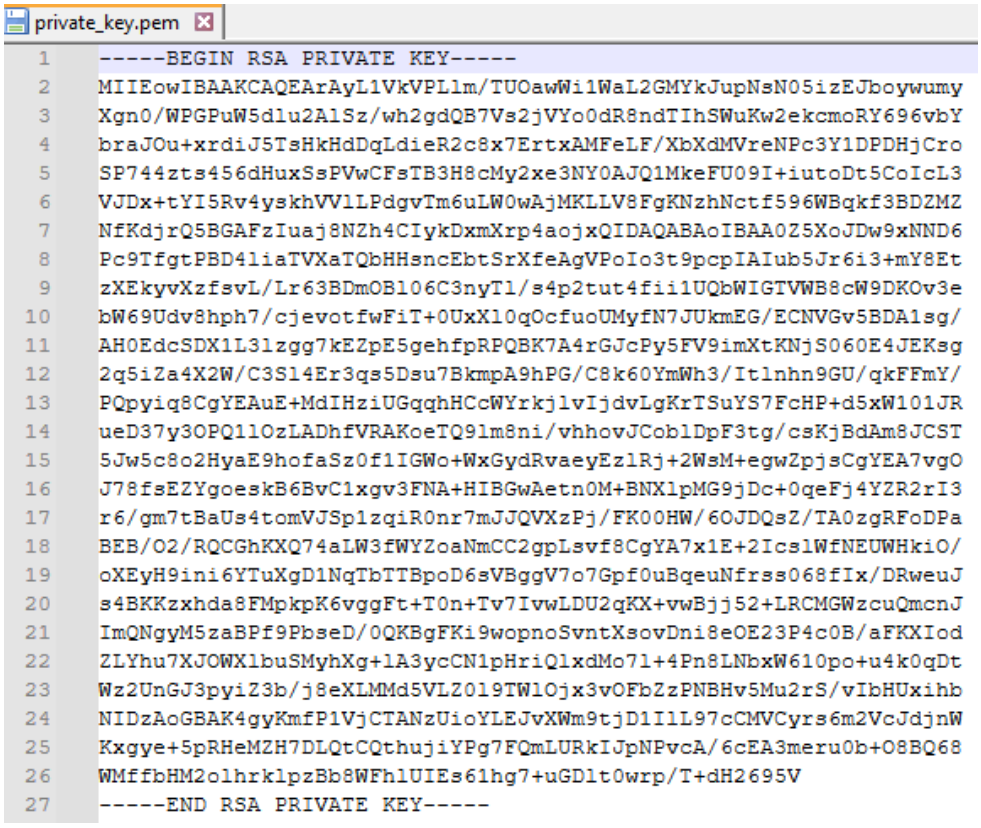


Рисунок 3.3 – Згенерований приватний ключ

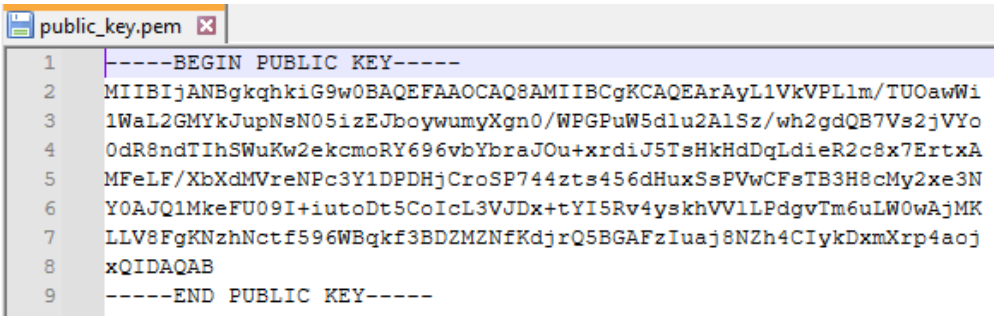


Рисунок 3.4 – Згенерований публічний ключ

Зміна ключів RSA дійсно може допомогти захистити інформаційну систему підприємства, особливо якщо є загроза компрометації або витоку даних. Це необхідно в таких випадках, як виявлення підозрілої активності під час аудиту безпеки, ризик НД, або злом. Заміна ключів може також бути пов’язана з впровадженням нових політик безпеки, підвищених криптографічних стандартів або вдосконаленням алгоритмів. У таких випадках всі дані, для шифрування яких використовувся старий ключ, не можуть бути розшифровані новим ключем, і користувачі повинні пройти повторну реєстрацію.

Алгоритм реєстрації користувачів (рисунок 3.5) включає наступні кроки:

– отримання даних з форми: ім'я користувача та пароль;

– перевірка унікальності отриманих даних. Відбувається пошук ID користувача у БД. Якщо користувач з таким іменем існує виводиться повідомлення про помилку реєстрації. Якщо ні, продовжити виконання.

– генерація «солі» - створення випадкового 512-бітного значення для унікального хешування пароля;

– хешування пароля за допомогою алгоритму PBKDF2 (SHA-256) з додаванням «солі»;

– шифрування хешу із застосуванням асиметричного алгоритму RSA для захисту даних, що зберігаються;

– зберігання даних в БД. Інформація зберігається у файлі stored_passwords та містить ID користувача, зашифрований

хеш пароля та сіль;

- виведення повідомлення про успішну реєстрацію.

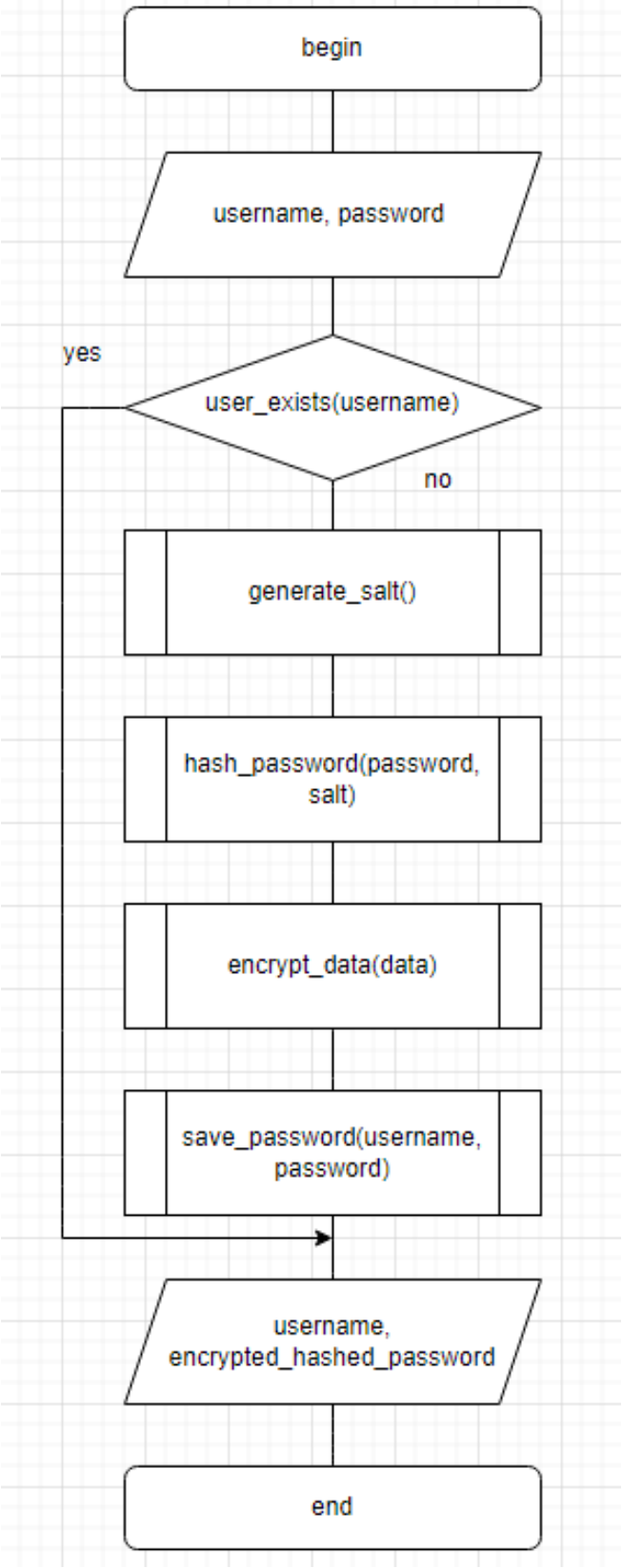


Рисунок 3.5 - Алгоритм реєстрації

Алгоритм автентифікації (рисунок 3.6) включає наступні кроки:

- отримання даних: ім'я та пароль користувача;
- перевірка існування користувача в БД. Якщо ні, вивести повідомлення про помилку. Якщо так, продовжити.
- 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 зберігаєтьсяв БД, і результат порівнюється з розшифрованим хешем пароля. Якщо дані співпадають, автентифікація успішна. Якщо ні, вивести повідомлення про помилку.

Для підвищення захисту даних від атак перебором реалізовано процедуру блокування користувача після кількох невдалих спроб. Для цього реалізована процедура зберігання кількості спроб автентифікації для ID користувача. Лічильник обнуляється в результаті вдалої спроби автентифікації. Якщо кількість помилок перевищує встановлене значення обліковий запис буде видалений з БД СКП або заблокований на певний час.

Користувач може змінити свій пароль після успішної перевірки старого пароля. Новий пароль хешується і шифрується, а інформація в файлі оновлюється. Алгоритм оновлення даних (рисунок 3.7) містить кроки:

- отримання даних з форми: ім’я користувача, старий пароль, новий пароль та підтвердження нового пароля;
- виконання перевірки існування користувача з таким іменем в БД;
- перевірка старого пароля, шляхом виконання процедури автентифікації. Якщо пароль правильний, продовжити. Якщо ні, вивести повідомлення про помилку.
- оновлення даних шляхом генерації нової солі для введеного пароля;
- хешування нового пароля із застосуванням нової солі для хешування нового пароля;

- шифрування нового хешу для його захисту з використанням RSA;
- оновлення даних шляхом заміни старої солі та хешу на нові у БД.

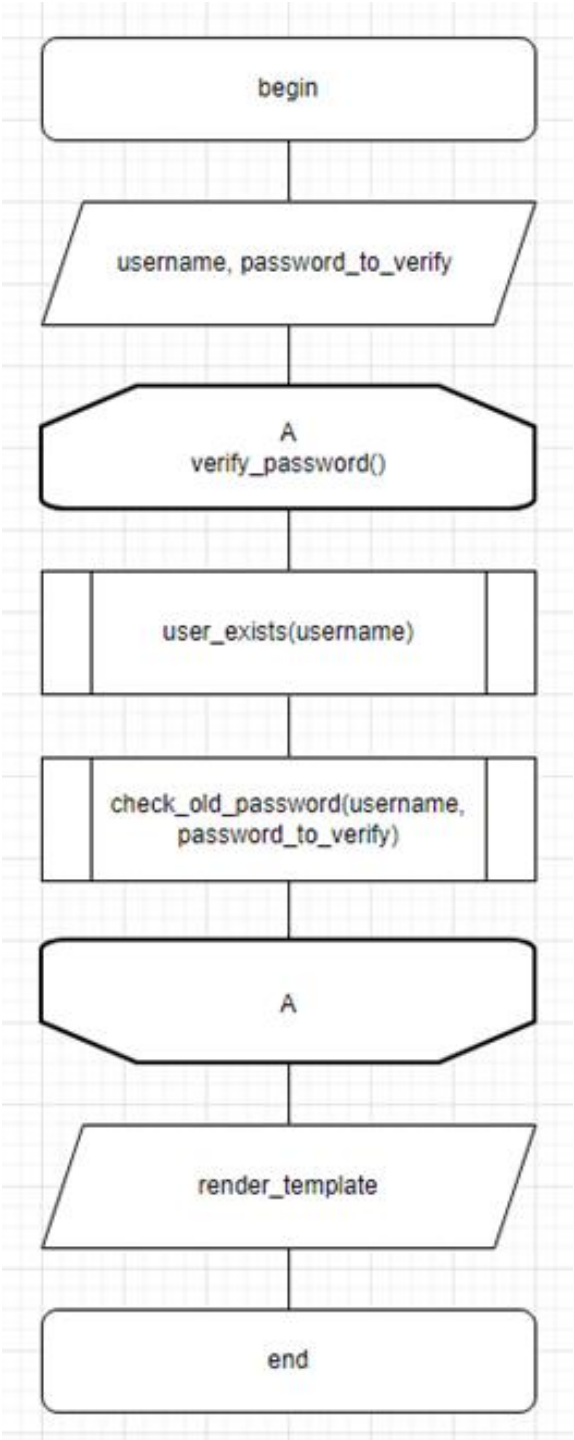


Рисунок 3.6 - Алгоритм автентифікації

В роботі проектованої СКП передбачена обробка помилок, зокрема неправильного формату пароля, помилки з'єднання з БД, а ткож можливість ведення журналу подій для відстеження спроб входу та реєстрації.

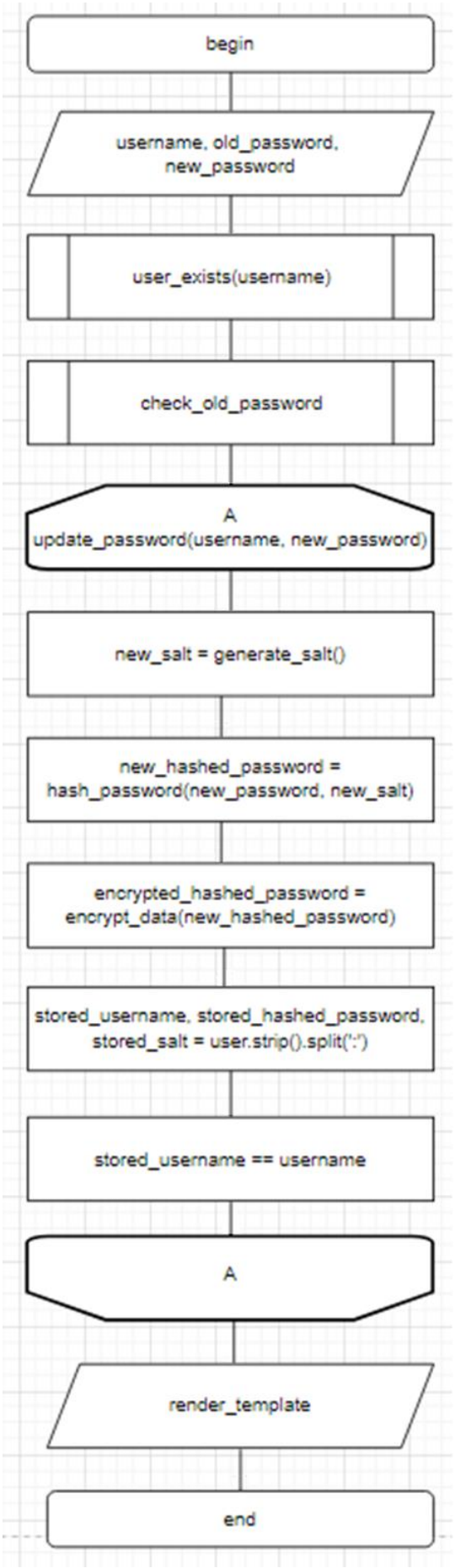


Рисунок 3.7 - Алгоритм оновлення даних

Хешування паролів забезпечує невідновлюваність даних та ганрантує їх безпечне зберігання. Під час автентифікації СКП хешує введений пароль та порівнює його із збереженим в БД хешем. Додавання «солі» підвищує безпеку паролів, захищаючи від атак словникового типу, бутфорс атак, повторного використання тощо.

Шифрування хешів паролів та «солі» перед зберіганням у БД забезпечує їх конфіденційність. Це ускладнює доступ до паролів у разі витоку даних, оскільки вміст залишається недоступним без відповідного ключа.

Запропоновані алгоритми реалізують безпечну систему реєстрації користувачів та управління паролями. Використання різних криптографічних методів забезпечує комплексний підхід до захисту даних для збереження конфіденційності, цілісності та доступності інформації.

При реалізації СКП параменти солі, хешу та ключів RSA впливають на безпеку системи та визначають необхідні обчислювальні ресурси. Для забезпечення оптимальних параметрів використовуються:

- розмір солі 128 біт - генерується за допомогою `os.urandom(16)`, що додає 16 випадкових байтів забезпечує унікальність хешів для однакових паролів;
- розмір хешу 256 біт - залежить від використовуваного алгоритму в даній реалізації використовується `PBKDF2` з хешуванням на основі `SHA-256. Виконання 100,000 ітерацій хешування ускладнює реалізацію атаки методом перебору;
- розмір ключів RSA 2048 біт - є стандартним розміром для RSA, генеруються за допомогою `RSA.generate(2048)`, та дозволяють забезпечувати достатній рівень безпеки

Ці параметри можуть змінюватись в залежності від потреб безпеки системи, проте зазначені значення відповідають стандартам для сучасних застосувань.

3.2 Реалізація системи керування паролями

Проектована СКП використовує шифрування прихованих паролів під час зберігання та передачі, що підвищує захист від НД. Система поєднує алгоритми хешування, шифрування та технік безпечного управління ключами для захисту облікових даних. Коли користувач входить в систему, його пароль ніколи не розкривається - замість цього він шифрується за допомогою алгоритму RSA. Цей прихований пароль захищає вашу систему від витоків, коли зловмисники крадуть БД паролів.

Програмна реалізація СКП наведена в додатку А. Код є серверною веб-програмою на основі Flask, що забезпечує функціонал реєстрації, перевірки пароля, оновлення даних та керування користувачами з використанням RSA шифрування та хешування паролів. Для реалізації використано останні версії бібліотек:

- Flask - для створення веб-сервера та обробки HTTP-запитів.
- os - для роботи з файловою системою (збереження ключів, паролів тощо).
- hashlib - для хешування паролів за допомогою алгоритму `SHA256`.
- binascii -для роботи з двійковими та текстовими даними (конвертація в шістнадцяткову систему).
- logging - для ведення журналу подій (логування).
- datetime - для роботи з датами і часом (використовується у файлах логів).
- Crypto.PublicKey.RSA, Crypto.Cipher.PKCS1_OAEP, Crypto.Signature.pkcs1_15 - для створення та використання RSA ключів, шифрування і підпису даних.

Основні функції включають:

- save_keys(); load_keys() - для зберігання та завантаження RSA-ключів;

- encrypt_data();decrypt_data() – для шифрування/дешифрування даних за допомогою ключів RSA відповідно;
- generate_salt() – функція генерації «солі» для хешування паролів;
- hash_password() - для хешування паролів із використанням солі;
- user_exists();check_old_password() – для перевірки існування в БД користувача та пароля;.
- save_user(); delete_user() - для реєстрації/видалення облікового запису;
- update_password() – для оновлення даних.

Основні маршрути:

- (`/`): - головна сторінка;
- (`/save`) - реєстрація нового облікового запису;
- (`/verify`) - перевірка правильності введених даних при автентифікації;.
- (`/update`) - сторінка оновлення даних;
- (`/update_password`) - обробка запиту на оновлення даних.

Програма також веде облік кількості спроб автентифікації та видаляє користувача, якщо перевищено максимальну кількість спроб.

Основною метою проектування є створення надійної СКП, яка не тільки захищає чутливу інформацію, але й забезпечує користувачам інтуїтивно зрозумілий інтерфейс (рисунок 3.8).

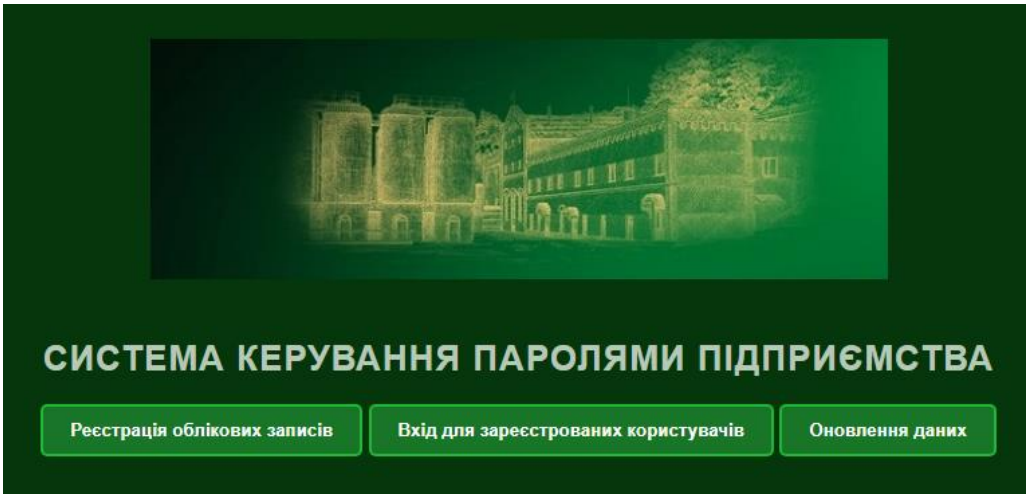


Рисунок 3.8 – Головна сторінка

Проектована система використовує HTML як основний засіб для побудови інтерфейсу користувача. Лістинг HTML-коду інтерфейсу користувача наведений в додатку Б. На рисунку 3.9 наведено форму реєстрації облікового запису.

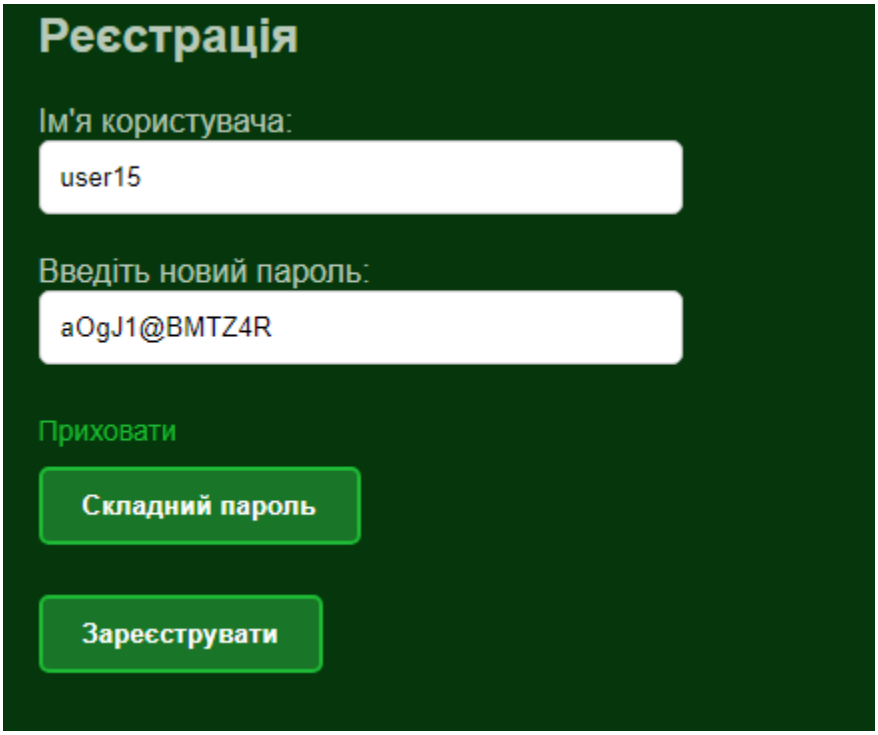


Рисунок 3.9 – Форма реєстрації

В проектовані системі передбачена можливість відобразити/приховати введені користувачем дані. При реєстрації СКП можна використати згенерований складний пароль або ввести значення, що відповідає вимогам до паролів в системі.

В результаті успішної реєстрації облікового запису дані зберігаються в БД системи (рисунок 3.10).

```
user116:7e104b88312288e0a6e6a1667e6893f3ab05e5369e8e0f649718b9961a009cf27d591001a5d81a2efe3df3dc1b7433dcd96eec287e4be2d8ebe283
user200:a9d0c35023579c1cb672b3eb3a1a8db64ee2a2e255c2f697fd04855b396ad9ee7b851d48803e45a2a4145b08ffe11d40487b1aba57f74d94d875e5
user201:85fc715dc7e6b30c9e78ee7a9760c65831c39b66c271e5c805a060e8abd9f67e22d2407c5bab651fd41c06aee87cc497f504a58bd93a95fdf3dfa4
user300:20d1e3964125029f7705f07c3eefec4d8b7f3aa43d9f1dccfefe4eeb50b8865a1142939085e7629d9c7bcab07838f0e0d746a3730cfafed70e4683
user202:1a244df5a52b71be5a3391b1efb799695eb2db900da5584680e797b3befe355266a2023784b73f3caafb7a760a7a7b7d4050977950679b89ced7d2
user500:bb270057a818d425da88a2affe016dca3715658b613bd3a1fc322eed84ec0d98da1d89cedce3e96f79adc25c0578192b8aafa57cfe95917fb65dfe
user001:538d4d5b49aedb86f2cd8bfc099b576b084cb99e13a6874ad6b8845608714f3e852b04840f53f8d30274a9e4ac3a11ab623dc41fd7d5e2bbaa5a34
user600:b981c844a2bdd7682bea777d0b06b99b02a2793db319ba401c5ed1eb97255b38cca66cdb086856f0549c607b9197afa516214798bde5786e95b1e2
user800:284bea6462936929431b8636d8d2f9fea7044d0a8c1f5f1f154e668630077c0c63705f35b7ed95dbbb44a409dbe44f8d017da76ff9f64955dcc145
user900:a16355a7244da24245b98b73ac30c990689062800cb2f45e8eafdb55b1207c788870cebcc2fe81d2b8ed4780fc78f56ae82988c11af293c8457769
user808:9be54b09cc08b05eaa06749898356631f06a28cc47ad4d92b734ae80aaab5dd819237da58d0228febabd0dba1537265744783d71eb1d7e9241c1c3
user1010:88baaada2469a8d1e56c1f4f6898ead47ec5003fd377a708c79c848c09c6c8e4eb86c0458ba3f5cb0ca31d1be7b464a899a05825b60f166e77eb6
user1011:a53330ac75b8005d7262857394b59190065fa2e0fc4a274f15791d178e5d821742c61a20bcb54115ee6387128bd693a2b4222ee12dd71fa796507
name16:2359b014d4d9ebd40e0fad16b53dcbee3d82b4e6b3e7b1c06e46da5e74110088c38fecd79f7e00b87510a7d648a31f3ec311364af3b96eb17d37705
user15:21a5770fcfdef2db6445a607341ccfca94124c61a5952ecbcd53539bf8346f9d2adcd1f86a3b2f3830a0416aec146d849d43bd486fee98452160129
```

Рисунок 3.10 – Фрагмент файлу stored_passwords

Інформація БД зберігається у форматі ID користувача:хеш:сіль. Наприклад в результаті реєстрації користувача з логіном user 500, отримаємо: user500:bb270057a818d425da88a2affe016dca3715658b613bd3a1fc322eed84ec0d98da1d89cedce3e96f79adc25c0578192b8aafa57cfe95917fb65dfeacee110f5ec6bb137cf4c83a6dec54629c46a28b07b9dd4c633ab13b75e658ea82470b63fb06e2e37c78a513a1ad63290e64600825ed96b3f7ecaa05cc4c1fd208d06c41ff14e9d414c90542d15b8f2cf87c3ad5e7af6699353c3a4c100f0ee7117c0d7514ab7932714744faa0671943af04841f57253610a67a97bad4992408b4e1b56b28ccbe853e9dcc51b99831897e01f7520249896003cc9fe3297e6b0beb3d1a2f54d6bf4ce6413a35d10be087857d922b9faeea4f91a48bbfa12d5590ff5df5403d:70abe29f4f463dd8d420da88feb24f31.

Форма для автентифікації наведена на рисунку 3.11.

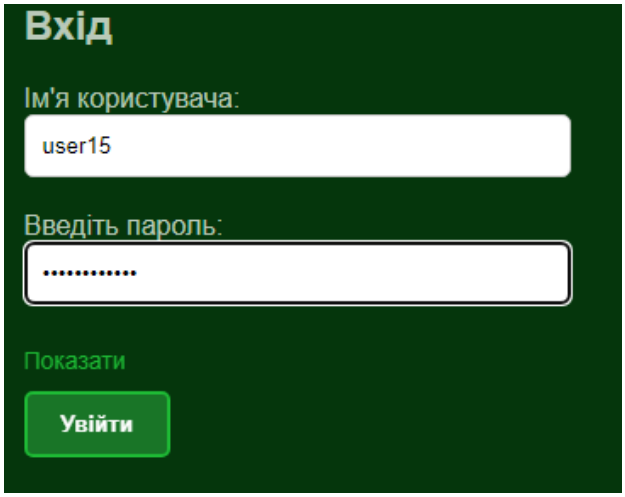
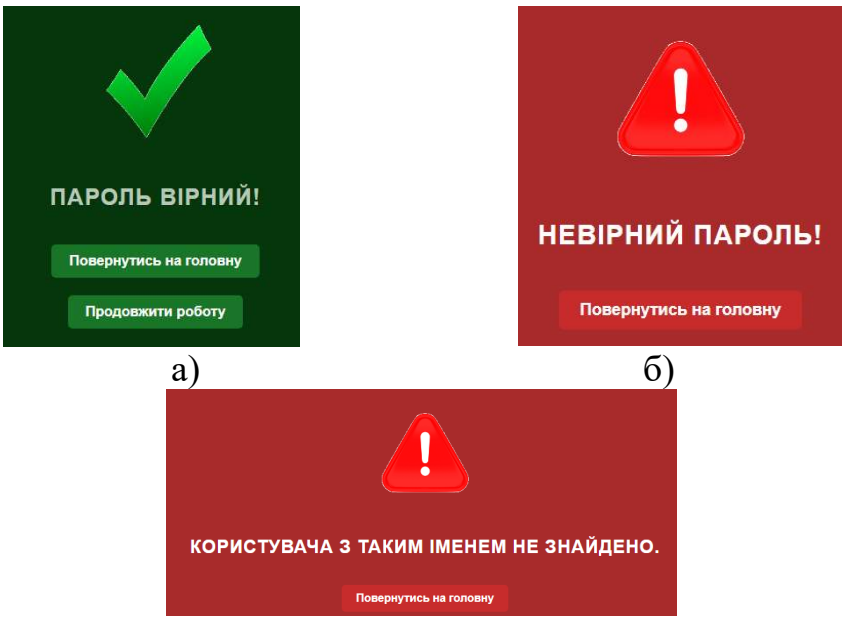


Рисунок 3.11 – Форма автентифікації

В результаті успішної перевірки користувач отримує доступ до ресурсів підприємства (рисунок 3.12а) в протилежному видаку в нього є можливість повторної автентифікації. На рисунку 3.12б наведено приклад сповіщень про невірно введений пароль та введений логін користувача, який не зареєстрований в системі (рисунок 3.12в)

Кількість спроб автентифікації визначається політикб безпеки та встановлюється під час налаштування СКП. У випадку перевищення максимальної кількості спроб облікові дані вважаються скомпрометованими та видаляються з БД.



а) б)

в)

Рисунок 3.12 – Сповіщення щодо результатів автентифікації

Рисунок 3.13 ілюструє сторінку оновлення даних облікового запису. Проектована система підтримує функцію автозаповнення, тобто автоматично пропонує варіанти для введення даних у поля вводу на основі раніше введених значень або доступних даних. Функція призначена для підвищення швидкості процесу введення даних і зручності користування СКП.

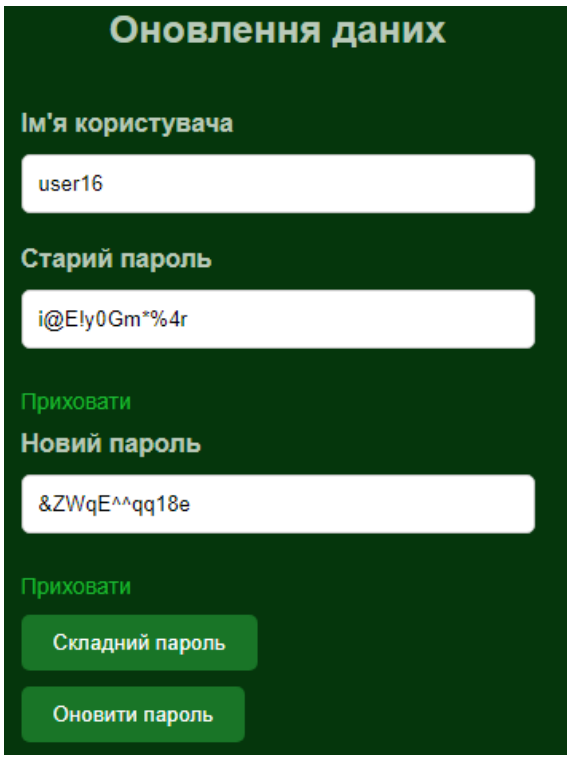


Рисунок 3.13 – Форма оновлення даних

В результаті успішного оновлення даних відбуваються зміни в БД системи (рисунок 3.14).

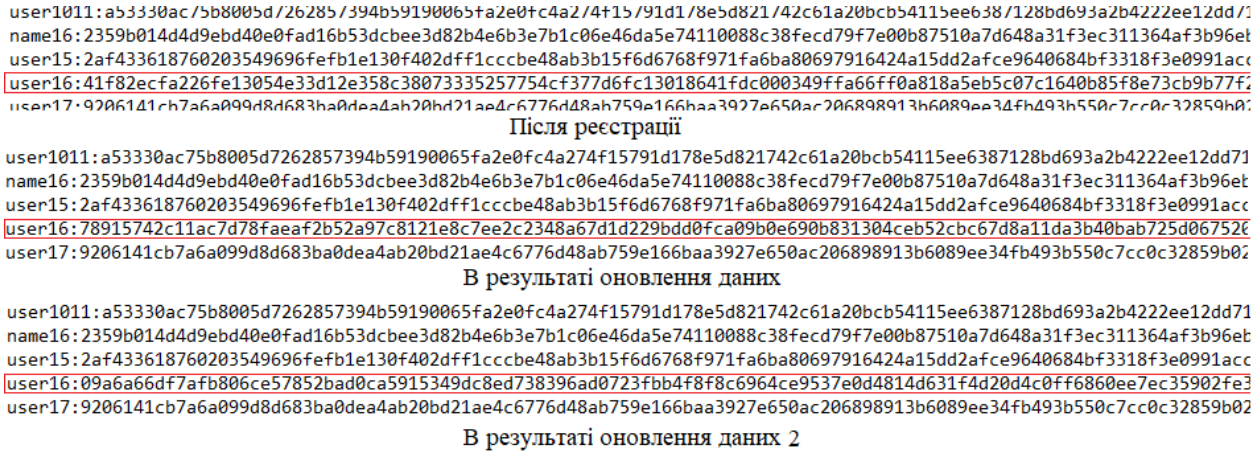


Рисунок 3.14 – Приклад відображення даних в БД при оновленні

У проектованій системі реалізовано функціонал ведення журналів подій, що фіксуються в консоль адміністратора (рисунок 3.15) і записуються у файл для подальшого аналізу (рисунок 3.16). Це забезпечує можливість моніторингу підозрілих дій. Log-файли створюються автоматично для кожного дня з іменем, що містить дату, наприклад, log_2024-10-19.txt.

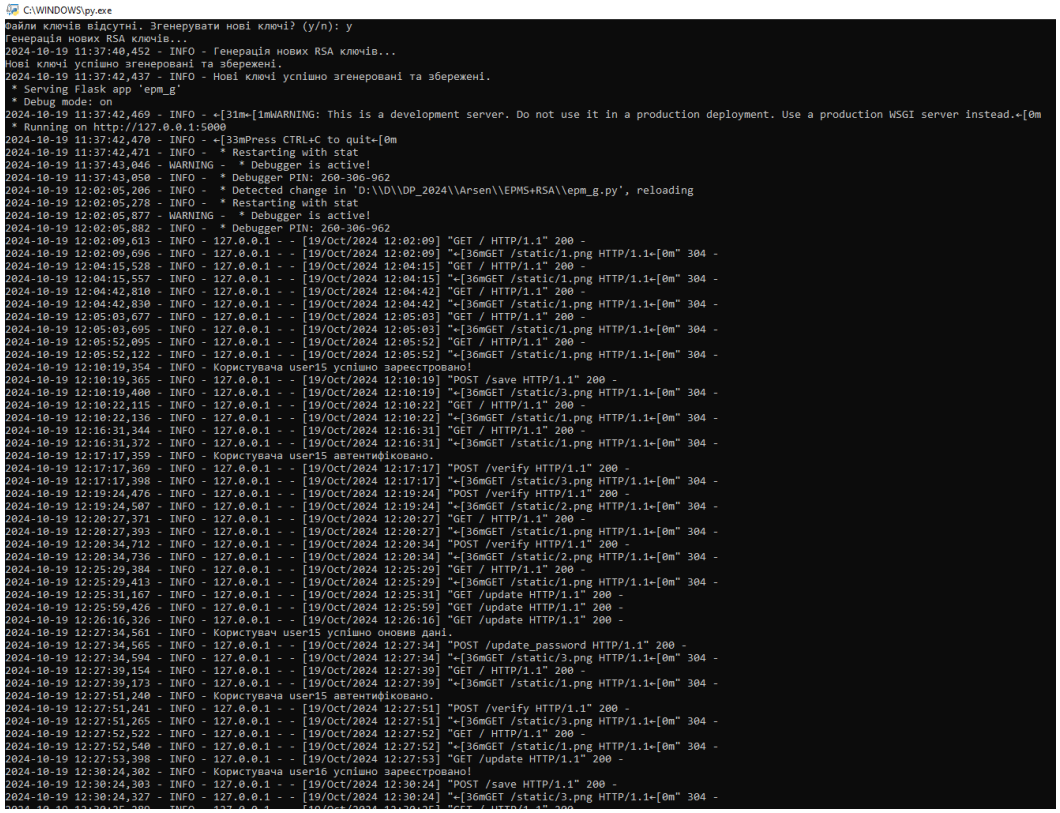


Рисунок 3.15 – Журнал поідй

Такий підхід дозволяє контролювати СКП, зокрема її безпеку, оскільки фіксуються такі події, як генерація нових ключів, реєстрація та автентифікація користувачів, успішне оновлення паролів, видалення користувачів після перевищення невдалих спроб входу та ін. Ведення журналів є важливим для аудиту системи в режимі реального часу і допомагає вирішувати проблеми, які можуть виникнути під час її використання.

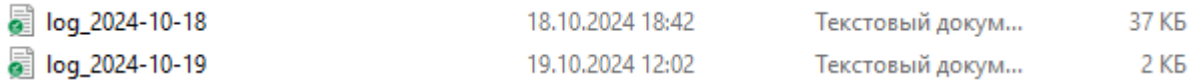


Рисунок 3.16 – Збережені log-файли

Результати тестування проектованої системи свідчать про те, що всі основні функції успішно виконуються. Паролі зберігаються в безпечному вигляді. Вони хешуються разом з сіллю та додатково шифруються, що ускладнює їх отримання. При автентифікації користувач може перевірити, чи правильно введено пароль, без розкриття фактичного пароля.

Розроблена СКП може бути використана у різних контекстах, де потрібна безпечна автентифікація користувачів, наприклад у додатках для управління проектами, корпоративних додатках або для внутрішніх портальних систем, де співробітники повинні автентифікуватися для доступу до ресурсів.

ВИСНОВКИ

Проведено аналіз існуючих інструментів та технологій управління паролями, класифіковано менеджери паролів, розглянуто їхні переваги та недоліки. Виявлено ефективні рішення, що можуть бути впроваджені в сучасних бізнес-процесах для підбищення рівня безпеки.

Проаналізовано методи шифрування, які застосовуються в системах керування паролями, зокрема алгоритми хешування, симетричного та асиметричного шифрування, а також криптографічні бібліотеки, що забезпечують надійний захист облікових даних. Визначено оптимальні підходи до захисту паролів від НД. Проведений аналіз дозволив сформувати вимоги до безпечних інструментів керування паролями

Розглянуто принципи роботи та функції СКП доступу до ресурсів, зокрема створення, зберігання, оновлення та видалення облікових записів з метою виявлення ключових аспектів ефективного управління паролями.

Досліджено алгоритми роботи МП, такі як зберігання та управління обліковими даними, реєстрації та автентифікації користувача, створення та редагування пароля та отримання даних з сервера, які забезпечили основу для подальшої розробки безпечних та ефективних алгоритмів управління паролями.

Досліджено вразливості в існуючих системах управління паролями, виявлено основні ризики, пов'язані з їх використанням, що дозволило виявити потенційні загрози, що можуть призвести до компрометації систем.

Розроблено структуру та алгоритм роботи проектованої системи керування паролями, реалізовано систему, яка відповідає сучасним вимогам інформаційної безпеки. Реалізована система дозволяє забезпечити підвищення рівня захисту корпоративних ресурсів, спростити процеси управління паролями та зменшити ризики компрометації даних.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дистанційна робота та її вплив на сучасне бізнес-середовище. [Електронний ресурс].- Режим доступу: https://bizmag.com.ua/bilshist-kompanii-prodovzhat-robotu-u-viddalenomu-rezhymi/

2. Цифрова трансформація бізнесу. [Електронний ресурс].- Режим доступу: https://techexpert.ua/digital-transformation-of-business/

3. Захарченко В. Переведення бізнесу на віддалену роботу: проблема чи вікно можливостей? [Електронний ресурс].- Режим доступу: https://pgrow.com.ua/blog/vladimir-zaharchenko/perevod-biznesa-na-udalennuyu-rabotu-problema-ili-okno-vozmozhnostey-1

4. Chatzoglou E., Kampourakis V., Tsiatsikas Z., Karopoulos G., Kambourakis G. Keep Your Memory Dump Shut: Unveiling Data Leaks in Password Managers. 2024. https://doi.org/10.1007/978-3-031-65175-5_5.

5. Курій Є. Дистанційна кібербезпека: як захистити інформацію під час віддаленого режиму роботи. [Електронний ресурс].- Режим доступу: https://mind.ua/openmind/20210952-distancijna-kiberbezpeka-yak-zahistiti-informaciyu-pid-chas-viddalenogo-rezhimu-roboti

6. Кібербезпека фірми під час дистанційної роботи: що компаніям потрібно пам’ятати? [Електронний ресурс].- Режим доступу: https://novarobota.ua/ua/articles-jobseeker/kiberbezopasnost-firmy-pri-distantsionnoy-rabote-chto-kompaniyam-nuzhno-pomnit-476

7. Як захистити свої персональні дані від кіберзлочинців. [Електронний ресурс].- Режим доступу: https://cyberpolice.gov.ua/article/yak-zaxystyty-svoyi-personalni-dani-vid-kiberzlochyncziv-dyvitsya-chergovu-seriyu-proyektu-kiberbezpekaua-7914/

8. Інформаційна безпека / за заг. ред. Ю.Я. Бобала та І.В. Горбатого / Львів : Видавництво Львівської політехніки, 2019. 580 с.

9. Гулак Г.М., Жильцов О.Б., Киричок Р.В., Коршун Н.В., Складанний П.М. Інформаційна та кібернетична безпека підприємства: підруч. / Г.М.

Гулак, О.Б. Жильцов, Р.В. Киричок, Н.В. Коршун, П.М. Складанний – Львів : Видавець Марченко Т.В., 2024. – 370 с.

10. 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.

11. Patel N., Kalra A. (2023). Secure Password Manager [Електронний ресурс].- Режим доступу: https://www.researchgate.net/publication/371012220_SECURE_PASSWORD_MANAGER

12. Padalia H., Patel H., Deshmukh A., Patil M., Kumar A., Kumar Nrip N. A Study on Password Manager: Users' Perspective / 2023 International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA), Bengaluru, India, 2023, pp. 72-75, https://doi.org/10.1109/CIISCA59740.2023.00024

13. Gautam A., Kumar Yadav T., Seamons K., Ruoti S. (2024) Passwords Are Meant to Be Secret: A Practical Secure Password Entry Channel for Web Browsers [Електронний ресурс].- Режим доступу: https://arxiv.org/pdf/2402.06159

14. Gallagher E. (2019). Choosing the Right Password Manager. Serials Review. 45. 1-4. 10.1080/00987913.2019.1611310.

15. 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.

16. Kolesnichenko P., Progonov D., Cherniakova V., Oliynyk A., Sokol O. Biometric-Based Password Management. 2023. https://doi.org/10.1007/978-3-031-47198-8_2.

17. Keeper [Електронний ресурс].- Режим доступу: https://www.keepersecurity.com/

18. Dashlane. [Електронний ресурс].- Режим доступу:

https://www.dashlane.com/]

19. Password. [Електронний ресурс].- Режим доступу: https://1password.com/

20. Зв'язка ключів iCloud. Настроювання та використання. [Електронний ресурс].- Режим доступу: https://www.cn.ua/news/apple/9383-zv-iazka-kliuchiv-icloud-nastroiuvannia-ta-vykorystannia.html

21. RoboForm. [Електронний ресурс].- Режим доступу: https://www.roboform.com/

22. NordPass. [Електронний ресурс].- Режим доступу: https://nordpass.com/

23. Zoho Vault. [Електронний ресурс].- Режим доступу: https://www.zoho.com/vault/

24. Passwarden. [Електронний ресурс].- Режим доступу: https://www.passwarden.com/

25. Bitwarden. [Електронний ресурс].- Режим доступу: https://bitwarden.com/

26. Enpass. [Електронний ресурс].- Режим доступу: https://www.enpass.io/

27. Sticky Password. [Електронний ресурс].- Режим доступу: https://www.stickypassword.com/

28. LastPass. [Електронний ресурс].- Режим доступу: https://www.lastpass.com/

29. RememBear. [Електронний ресурс].- Режим доступу: https://www.remembear.com/

30. Passbolt. [Електронний ресурс].- Режим доступу: https://www.passbolt.com/

31. Baskar K., Muthumanickam K., Vijayalakshmi P., Sengottaiyan K. A Strong Password Manager Using Multiple Encryption Techniques. Journal of The Institution of Engineers (India): Series B. 2024. https://doi.org/10.1007/s40031-024-01144-6.

32. Password Management. [Електронний ресурс].- Режим доступу: https://www.netiq.com/documentation/privileged-account-manager-42/npam_admin/data/t4dywhxl25r9.html

33. Carr M., Shahandashti S. Revisiting Security Vulnerabilities in Commercial Password Managers. 2020. https://doi.org/10.1007/978-3-030-58201-2_18.

34. Gautam A. Enhancing security and usability in password-based web systems through standardized authentication interactions. [Електронний ресурс].- Режим доступу: https://userlab.utk.edu/files/papers/ruoti/2024/gautam2024enhancing.pdf

35. Pei T., Kasmin I., Marlia Z., Vasudavan H. Browser-Based Password Manager Using Tokenization. International Journal of Data Science and Advanced Analytics. 4. 236-241. 2023. https://doi.org/10.69511/ijdsaa.v4i0.171.

36. Password Managers: Under the Hood of Secrets Management. [Електронний ресурс].- Режим доступу: https://www.ise.io/casestudies/password-manager-hacking/