ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ МЕНЕДЖЕРІВ ПАРОЛІВ

Ганзя Р.С., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному цифровому середовищі проблема безпечного зберігання облікових даних стає дедалі актуальнішою, адже кількість сервісів і акаунтів постійно зростає. Користувачі змушені взаємодіяти з великою кількістю інформаційних систем, що потребує створення та використання унікальних і складних паролів. Менеджер паролів – це окрема програма або частина більшого середовища (наприклад, браузера), що відповідає за керування важливими даними, як-от логіни та паролі облікових записів або PIN-коди. Використання такого інструменту значно спрощує взаємодію з інформаційними системами, оскільки позбавляє необхідності запам'ятовувати велику кількість облікових даних. Крім того, програми цього типу забезпечують зберігання інформації у зашифрованому вигляді, що підвищує рівень її захисту від несанкціонованого доступу [1]. Додатково багато сучасних рішень пропонують генерацію стійких паролів та автоматичне заповнення форм, що сприяє підвищенню загальної кібергігієни користувачів.

Водночас менеджери паролів мають не лише переваги, але й певні ризики, зокрема пов'язані з компрометацією головного пароля або вразливостями у програмному забезпеченні. Централізація облікових даних в одному сховищі може створювати єдину точку відмови, що робить такі рішення привабливою ціллю для атак. У разі успішної атаки зловмисник може отримати доступ до значного обсягу конфіденційної інформації. Також важливим аспектом є довіра до розробника та механізмів шифрування, які використовуються у конкретному продукті. Крім того, слід враховувати ризики, пов'язані з використанням хмарної інфраструктури, зокрема можливість атак на серверну частину або перехоплення даних під час синхронізації.

Метою доповіді є здійснення порівняльного аналізу архітектури, методів шифрування та зручності сучасних менеджерів паролів (Bitwarden, 1Password та KeePassXC) для виявлення їхніх недоліків та формування базових вимог до розробки власного оптимізованого програмного рішення.

В доповіді наводяться результати аналізу обраних програмних рішень, що демонструють різні підходи до управління конфіденційними даними.

Bitwarden пропонує надійний баланс між прозорістю та зручністю. Цей продукт має відкритий вихідний код, підтримує хмарну синхронізацію та дозволяє розгортання на власному локальному сервері, що робить його привабливим як для індивідуальних, так і для корпоративних користувачів [2]. Додатково він використовує сучасні алгоритми шифрування та механізми захисту, включаючи двофакторну автентифікацію.

1Password є комерційним рішенням із закритим кодом, яке фокусується на максимальному комфорті. Програма відзначається високим рівнем

інтеграції з операційними системами, бездоганним користувацьким інтерфейсом та розширеними функціями для сімейного або командного використання [4]. Він також реалізує додаткові механізми захисту, такі як секретний ключ (Secret Key), що підвищує стійкість до атак навіть у разі компрометації основного пароля.

Водночас відсутність відкритого коду може обмежувати можливість незалежної перевірки додатку.

Натомість KeePassXC кардинально відрізняється своїм підходом до зберігання – це повністю локальна програмне рішення з відкритим кодом. Воно залишає синхронізацію та повний контроль над зашифрованим файлом бази даних виключно за користувачем [3]. Такий підхід забезпечує максимальний рівень контролю над даними, проте потребує від користувача додаткових знань для організації резервного копіювання та синхронізації між пристроями.

Основні відмінності існуючих рішень наведено у таблиці 1.

Таблиця 1 – Основні характеристики менеджерів паролів

Характеристика	**Bitwarden**	**1Password**	**KeePassXC**
Вихідний код	Відкритий	Закритий	Відкритий
Зберігання даних	Хмарне / Локальне	Хмарне	Локальне
Синхронізація	Автоматична	Автоматична	Ручна (через сторонні сервіси)
Вартість	Є безкоштовна версія	Платна підписка	Повністю безкоштовно

Порівняння цих рішень свідчить про відсутність абсолютно універсального продукту: кожен має свої обмеження щодо безпеки, контролю або зручності. Це обґрунтовує доцільність розробки нового менеджера паролів, який зможе ефективно поєднати гнучкість і безпеку локального контролю (як у KeePassXC) із сучасним інтерфейсом та зручністю автоматичної синхронізації (як у комерційних аналогах).

Список літератури

1. Рикова В. Для чого потрібен менеджер паролів і який обрати. URL: https://ms.detector.media/kiberbezpeka/post/29917/2022-07-26-dlya-chogo-potriben-menedzher-paroliv-i-yakyy-obraty/ (дата звернення: 8.03.2026).

2. Best password manager for business, enterprise & personal | bitwarden. Bitwarden. URL: https://bitwarden.com/ (дата звернення: 8.03.2026).

3. KeePassXC password manager. KeePassXC Password Manager. URL: https://keepassxc.org/ (дата звернення: 8.03.2026).

4. Passwords, secrets, and access management | 1password. Passwords, Secrets, and Access Management | 1Password. URL: https://1password.com/ (дата звернення: 8.03.2026).