УДК 004.056

М. І. Ткачук
В. В. Лукічов

МЕТОД ДЛЯ ЗАХИСТУ ПАРОЛІВ

Вінницький національний технічний університет

Анотація

У роботі запропоновано метод безпечного менеджера паролів на основі використання апаратного ключа безпеки YubiKey. Розглянуто переваги застосування фізичного токена для збереження та автозаповнення паролів, що забезпечує високий рівень захисту від несанкціонованого доступу, фішингу та компрометації облікових даних. Описано алгоритм роботи системи, у якій криптографічні операції та автентифікація виконуються безпосередньо на YubiKey, а також окреслено потенційні виклики, пов'язані з інтеграцією апаратного ключа, зручністю використання та масштабованістю.

Ключові слова: YubiKey, менеджер паролів, кібербезпека, апаратна автентифікація, криптографія.

Abstract

The paper proposes a secure password manager method based on the use of the YubiKey hardware security key. It considers the advantages of using a physical token for storing and autofilling passwords, which provides a high level of protection against unauthorized access, phishing, and account compromise. The algorithm of the system, in which cryptographic operations and authentication are performed directly on YubiKey, is described, and potential challenges related to hardware key integration, usability, and scalability are outlined.

Keywords: YubiKey, password manager, cybersecurity, hardware authentication, cryptography.

Вступ

У сучасному цифровому світі кібербезпека є однією з ключових проблем, з якими стикаються користувачі та організації. Зростання кількості онлайн-сервісів та необхідність запам'ятовування великої кількості паролів призводить до використання слабких або повторюваних комбінацій, що значно підвищує ризик компрометації даних. Традиційні менеджери паролів, які зберігають дані у зашифрованому вигляді, проте покладаються лише на програмні методи автентифікації, залишаються вразливими до фішингу, крадіжки майстер-пароля або компрометації пристрою.

Використання апаратних ключів безпеки YubiKey пропонує новий підхід до управління паролями та захисту доступу. YubiKey забезпечує апаратну автентифікацію та криптографічний захист, ізоляцію секретних ключів у фізичному пристрої та стійкість до атак, спрямованих на перехоплення чи підробку даних. Завдяки підтримці протоколів FIDO2, U2F, OTP та PIV, апаратний ключ дозволяє суттєво підвищити рівень безпеки при вході в менеджер паролів, шифруванні збережених даних та підтвердженні операцій.

Результати дослідження

Запропонований підхід до створення безпечного менеджера паролів із використанням апаратного ключа YubiKey було проаналізовано з точки зору безпеки, продуктивності та ефективності управління даними. Основні переваги такого рішення включають апаратну автентифікацію, ізоляцію криптографічних ключів на фізичному пристрої, високий захист від фішингу та перехоплення даних, а також істотне зниження ризику несанкціонованого доступу навіть у разі компрометації комп'ютера користувача. Водночас існують певні виклики, зокрема необхідність наявності фізичного токена, можливі труднощі з його перенесенням між пристроями, а також залежність від підтримки відповідних протоколів сервісами. Загальний алгоритм роботи методу зображено на рис. 1.

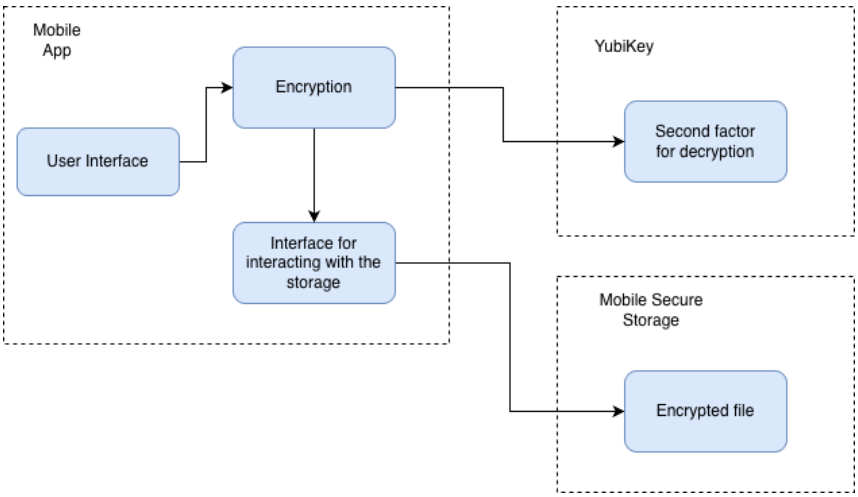

Рис 1. Загальний алгоритм роботи методу

Для оцінки ефективності менеджера паролів на основі YubiKey було проведено порівняльний аналіз його характеристик із традиційними програмними менеджерами паролів. Основні результати наведено в таблиці 1.

Таблиця 1. Порівняння традиційних та менеджерів, що використовують YubiKey

Параметр	**Традиційний менеджер паролів**	**Менеджер паролів із YubiKey**
Централізація	Централізоване сховище	Апаратний ключ (FIDO2/U2F/OTP)
Ризик злому	Високий (атаки на сервер)	Низький (паролі не залишають пристрою)
Прозорість	Низька (дані у приватній базі)	Висока (прив’язка до домену)
Швидкість доступу	Висока	Висока (вставлення ключа)
Вартість	Безкоштовно / передплата	Ціна апаратного ключа
Можливість відновлення	Є (через адміністратора)	Через резервний Yubikey
Додаткові можливості	Авто-заповнення, генерація паролів	Апаратні криптоопераії, багатофакторна автентифікація

Аналіз показав, що інтеграція YubiKey у менеджер паролів забезпечує значно вищий рівень безпеки порівняно з традиційними рішеннями, особливо у сфері захисту від фішингу та крадіжки облікових даних. Разом із тим важливими напрямами подальших досліджень залишаються підвищення зручності використання, оптимізація механізмів відновлення доступу та забезпечення сумісності з широким спектром програмних платформ і онлайн-сервісів.

Висновки

Запропонований метод для захисту паролів із використанням апаратного ключа YubiKey забезпечує високий рівень безпеки та захисту конфіденційних даних завдяки апаратній автентифікації, ізоляції криптографічних ключів та неможливості їхнього витоку з пристрою. На відміну від традиційних програмних рішень, YubiKey мінімізує ризики, пов’язані з фішингом, перехопленням майстер-пароля чи компрометацією пристрою, оскільки доступ до менеджера паролів вимагає фізичної присутності користувача та підтверджується апаратним токеном. Підтримка протоколів FIDO2, U2F та OTP дозволяє надійно захищати процеси автентифікації та підвищує ефективність управління доступом.

Водночас існують певні виклики, зокрема необхідність наявності фізичного ключа, потреба у резервному пристрої для відновлення доступу та залежність від підтримки відповідних стандартів з боку онлайн-сервісів. Для широкого впровадження таких систем важливо оптимізувати механізми

відновлення доступу, забезпечити сумісність з різними платформами та підвищити зручність використання апаратних ключів у повсякденній роботі.

Перспективними напрямами подальших досліджень є вдосконалення алгоритмів взаємодії менеджера паролів із YubiKey, розробка гібридних рішень із використанням кількох факторів автентифікації, а також створення інтерфейсів, які забезпечать максимальну зручність, інтуїтивність та доступність використання апаратного ключа в системах керування доступом.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yubico. The YubiKey. URL: https://www.yubico.com/. (Last accessed: 16.11.2025).
2. В. І. Гаврилюк, П. М. Денисюк, Ю. В. Лисенко. Криптографічні методи захисту даних: Навчальний посібник. Київ: Наукова думка, 2020. 250 с. (Last accessed: 16.11.2025).
3. ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання. Київ: Держспоживстандарт України, 2007. 47 с. (Last accessed: 16.11.2025).

Ткачук Максим Ігорович — студент групи 1БС-24м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: max200325622@gmail.com.
Лукічов Віталій Володимирович – к. т. н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Maksym Tkachuk — student of 1БС-24м group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: max200325622@gmail.com.
Lukichov Vitalii – Ph.D., Associate Professor, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: lukichov.vitalyi@vntu.edu.ua.