УДК 004.056.52

А. О. Лівандовська
Ю. В. Баришев

АНАЛІЗ ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ PASSKEY

Вінницький національний технічний університет

Анотація

Досліджено роль традиційних паролів на етапі автентифікації користувачів та проаналізовано їх основні вразливості. Проведено дослідження альтернативних варіантів входу в обліковий запис, таких як безпарольна автентифікація на основі технології Passkey. Визначено технічну різницю між резидентними та нерезидентними ключами, що базується на методах генерації та зберігання конфіденційної інформації необхідної для реєстрації та вході в систему, можливих вразливостей та доступу до них за допомогою порівняльного аналізу.

Ключові слова: резидентний, нерезидентний, технологія passkey, протокол FIDO2, WebAuthn

Abstract

The role of traditional passwords in the user authentication process was examined, and their main vulnerabilities were analyzed. A study was conducted on alternative methods of logging into an account, such as passwordless authentication based on Passkey technology. The technical difference between resident and non-resident keys was identified, based on the methods of generating and storing the confidential information required for registration and system login, as well as potential vulnerabilities and access to them, through a comparative analysis.

Keywords: resident, non-resident, passkey technology, protocol FIDO2, WebAuthn

Вступ

В умовах зростання кіберзагроз традиційні методи автентифікації демонструють низький рівень захисту через масове використання користувачами ідентичних паролів, що створює ризик несанкціонованого доступу до конфіденційних даних облікового запису у разі зламу одного з них. Технологічним рішенням став стандарт FIDO2 та розроблена на його основі технологія passkey, що забезпечує перехід до безпарольного входу користувачів.

Метою даного дослідження є покращення рівня захисту автентичності інформації шляхом визначення особливостей застосування технології passkey.

Результати дослідження

Паролі вже давно є стандартною практикою для захисту конфіденційних даних, але, як показують численні дослідження, вони мають багато проблем, таких як: повторне використання в різних сервісах, вразливість до витоків даних, низька складність і, як наслідок, легкість вгадування тощо [1]. Протокол FIDO2 вирішує цю проблему можливістю безпарольного входу, що реалізується за допомогою двох основних компонентів, на яких він ґрунтується [2]:

- WebAuthn [4] – це інтерфейс прикладного програмування (API), який дозволяє вебзастосункам і браузерам взаємодіяти з автентифікаторами FIDO2 для реєстрації та автентифікації користувачів;
- CTAP [5] визначає, як клієнт (браузер або операційна система) спілкується з автентифікатором FIDO (наприклад, зовнішнім USB-ключем безпеки, смартфоном або вбудованим біометричним модулем).

Завдяки цим двом компонентам було реалізовано можливість безпарольного входу в обліковий запис, а саме технологію Passkey. Вона не просто реалізовує цей стандарт, а стає безпосереднім учасником процесу автентифікації, забезпечуючи безпечне зберігання конфіденційних ключів замість традиційних паролів.

Passkey є реалізацією резидентного ключа, що дає можливість стороні, що довіряє, спробувати використати облікові дані на автентифікаторі без надання користувачем ідентифікатора користувача [3]. Це значно спрощує процес входу, адже автентифікатор самостійно пропонує відповідний

обліковий запис для даного сервісу. Також існують нерезидентні ключі, що безпосередньо не є ключами доступу в сучасному розумінні Passkey, адже не мають змоги запам'ятовувати ідентифікатори користувачів у власній пам'яті, а лише генерують відповідні криптографічні підписи кожного разу, за потреби.

Для системного аналізу відмінностей між технологіями у таблиці 1 наведено порівняльну характеристику резидентних та нерезидентних ключів за ключовими технічними та функціональними можливостями.

Таблиця 1 – Порівняння резидентних та нерезидентних ключів доступу

Критерії	Резидентні	Нерезидентні
Яка мета створення?	Створення безпарольної автентифікацію	Додаткова перевірка особи
Місце зберігання основної інформації	На автентифікаторі	Не мають місця зберігання
Кількість можливих ключів	Залежно від розміру пам'яті	Необмежений
Умови генерації ключів	На основі випадкових чисел	Детерміновані
Вразливість	Втрата ключа	Теоретично компанія виробник може знати Master Key

Отже, резидентні ключі є більш зручними, оскільки дозволяють вхід без введення логіна, але мають обмеження у вигляді обмеженого обсягу пам'яті, тоді як нерезидентні можуть підтримувати необмежену кількість облікових записів без потреби зміни пристрою.

Таким чином, вибір між цими двома типами ключів залежить від зручності для користувача та технічних ресурсів автентифікатора.

Висновок

У підсумку, можна стверджувати, що новітні способи захисту облікових записів є досить прогресивними та стійкими до таких атак, як фішинг, «людина посередині», витік бази даних сервера, вгадування та інші. Основними проблемами, що перешкоджають масовому впровадженню ключів доступу, є невідповідне сприйняття технології користувачами [1] та непідтримка протоколу більшістю розробників вебсайтів, що унеможливлює повну інтеграцію цієї технології.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Matzen et al. Challenges and Potential Improvements for Passkey Adoption–A Literature Review with a User-Centric Perspective. *Applied Sciences*. 2025. 15(8), 34 p. URL: https://www.mdpi.com/2076-3417/15/8/4414 (last accessed: 15.03.2026).
2. Oleg Naumenko. Єдиний шлях – змінити всю модель безпеки. Як ми створили застосунок для безпарольної багатофакторної автентифікації. *DOU*. URL: https://dou.ua/forums/topic/55193/ (дата звернення: 15.03.2026).
3. Discoverable vs non-discoverable credentials: // Yubico Developers. URL: https://developers.yubico.com/Passkeys/Passkey_concepts/Discoverable_vs_non-discoverable_credentials.html (last accessed: 15.03.2026).
4. W3C Recommendation. Web Authentication: An API for accessing Public Key Credentials. Level 2. URL: https://www.w3.org/TR/webauthn/ (last accessed: 15.03.2026).
5. CTAP 2.2 Proposed Standard. Client to Authenticator Protocol (CTAP). Proposed July 14, 2025. *FIDO Alliance*. URL: https://fidoalliance.org/specs/fido-v2.2-ps-20250714/fido-client-to-authenticator-protocol-v2.2-ps-20250714.pdf (last accessed: 15.03.2026)

Лівандовська Анастасія Олегівна – студентка групи 1БКС-23Б, кафедри захисту інформації факультету інформаційних технологій комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: anastasialivandovska@gmail.com

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua

Livandovska Anastasiia Olehivna – student of group 1BKS-23B, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: anastasialivandovska@gmail.com

Yurii Baryshev Volodymyrovych – PhD, associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua