

ВИКОРИСТАННЯ МОБІЛЬНИХ ДОДАТКІВ- АУТЕНТИФІКАТОРІВ ДЛЯ АВТОРИЗАЦІЇ У БАНКІВСЬКІ ДОДАТКИ

¹ Вінницький національний технічний університет

Анотація

Було розглянуто принципи роботи та переваги використання мобільних аутентифікаторів порівняно з традиційними методами авторизації. А також досліджено технічні аспекти інтеграції таких додатків у банківські системи та їхній вплив на безпеку та зручність користування.

Ключові слова: мобільні аутентифікатори, традиційні методи авторизації, інтеграція, банківські системи, безпека.

Abstract

The operational principles and advantages of using mobile authenticators compared to traditional authentication methods were examined. Additionally, the technical aspects of integrating such applications into banking systems and their impact on security and user convenience were investigated.

Keywords: mobile authenticators, traditional authentication methods, integration, banking systems, security.

Вступ

У сучасному світі зростає популярність мобільних додатків-аутентифікаторів, які використовуються для забезпечення безпеки при авторизації в різних системах, зокрема, у банківських додатках.

Вони дозволяють підвищити рівень захисту від несанкціонованого доступу та зловживань. Використання мобільних аутентифікаторів в банківських системах стає необхідністю у зв'язку зі зростанням кількості кіберзагроз та потребою у надійному захисті клієнтської інформації. Зокрема, у сфері фінансових послуг, де важливість забезпечення конфіденційності та цілісності даних є надзвичайно великою, мобільні аутентифікатори стають невід'ємною складовою безпечних та надійних банківських систем. Їхнє впровадження допомагає уникнути фінансових втрат, шахрайства та інших загроз, що можуть стати причиною серйозних проблем як для користувачів, так і для фінансових установ.

Цілісність і безпека особистих фінансових даних досить актуальні у сучасному цифровому середовищі, де кіберзлочинці намагаються здійснювати атаки та отримувати несанкціонований доступ до фінансових ресурсів. Тому, дослідження та розгляд можливостей використання мобільних аутентифікаторів у банківських додатках стає вельми актуальним та важливим завданням в сучасному світі.

Результати дослідження

Проведене дослідження виявило, що мобільні аутентифікатори виявляються дієвим та надійним засобом забезпечення безпеки під час авторизації користувачів у банківських та інших системах. Принцип роботи цих додатків, який базується на генерації унікальних одноразових кодів(ТОТР)[1] або використанні біометричних даних, забезпечує високий рівень захисту від несанкціонованого доступу та зловживань(рисунок 1).

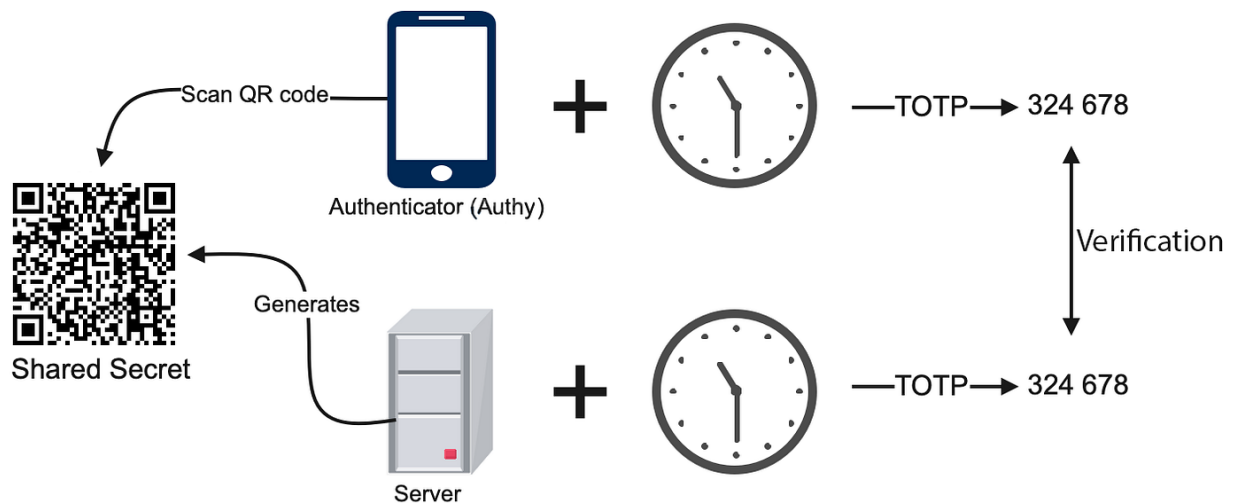


Рис. 1 – Принцип роботи мобільних додатків-аутентифікаторів

Аналіз наявних мобільних аутентифікаторів показав, що кожен з них має свої особливості та переваги. Наприклад, Google Authenticator[2] відомий своєю простотою та швидкістю генерації кодів, в той час як Authy[3] забезпечує можливість синхронізації з кількома пристроями для зручності користувачів.

Огляд переваг мобільних аутентифікаторів підкреслив їхню високу ефективність у захисті конфіденційності та безпеки особистих даних. Зокрема, вони забезпечують:

1. Додатковий шар захисту: Використання одноразових кодів або біометричних даних створює додатковий бар'єр для несанкціонованого доступу.
2. Зручність використання: Користувачам не потрібно запам'ятовувати складні паролі, що полегшує процес авторизації.
3. Можливість блокування доступу: Деякі аутентифікатори мають функцію блокування доступу в разі виявлення підозрілих дій.
4. Розширені функціональність: Деякі додатки підтримують синхронізацію та мають інші розширені функції для зручності користувачів.

Проте, наявність деяких недоліків також була виявлена під час дослідження:

1. Залежність від мобільного пристрою: Використання аутентифікатора передбачає доступність мобільного пристрою, що може бути незручно у разі втрати або поломки пристрою.
2. Можливість блокування доступу: В деяких випадках, втрата доступу до аутентифікатора може призвести до необхідності відновлення доступу до системи, що може бути часо- та ресурсозатратним процесом.

Висновки

Мобільні аутентифікатори представляють собою потужний та ефективний інструмент для захисту фінансових та особистих даних користувачів. Їхня висока безпека та зручність використання роблять їх популярними серед користувачів банківських та інших онлайн-систем. Однак, необхідно враховувати і недоліки цих додатків, такі як залежність від пристрою та можливість блокування доступу в разі втрати доступу до аутентифікатора.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. TOTP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.twilio.com/docs/glossary/totp>.
2. Google Authenticator [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchsecurity/definition/Google-Authenticator>.
3. Authy [Електронний ресурс] – Режим доступу до ресурсу: <https://www.twilio.com/docs/verify/authentication-channels>.

Ткачук Олексій Олександрович – студент групи ІАКІТР-23м, кафедра автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: oleksii.tkachuk878@gmail.com

Богач Ілона Віталіївна – к.т.н., доцент кафедри автоматизації та інтелектуальних інформаційних технологій, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м.Вінниця, e-mail: ilona.bogach@gmail.com

Тkachuk Oleksii Oleksandrovych – student of IACITR-23M group, Department of Automation and Intelligent Information Technologies, Faculty of Intelligent Information Technology and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksii.tkachuk878@gmail.com

Bogach Ilona Vitaliivna – Associate Professor of Automation and Intelligent Information Technologies, Faculty of Computer Systems and Automatics Vinnytsia National Technical University, Vinnytsia, e-mail: ilona.bogach@gmail.com.