Пирч О.В., асистент
Рак І.І., здобувач
Шемчук У.А., здобувач
Тітова В.Ю., к.т.н., доцент
Хмельницький національний університет

МЕТОД ПІДВИЩЕННЯ СТІЙКОСТІ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ЗА РАХУНОК КОМБІНОВАНИХ СХЕМ АУТЕНТИФІКАЦІЇ

Електронний цифровий підпис (ЕЦП) є важливим інструментом забезпечення автентичності, цілісності та доступності електронних документів. Проте сучасні загрози у сфері кібербезпеки вимагають удосконалення методів захисту криптографічних ключів та підвищення надійності процесу аутентифікації користувачів [1].

У даному дослідженні запропоновано підхід до підвищення стійкості ЕЦП шляхом застосування комбінованих схем аутентифікації, зокрема контекстуальної аутентифікації у поєднанні із біометрією, та впровадження штучного інтелекту для порівняння біометричних даних користувачів.

Контекстуальна аутентифікація [2] передбачає аналіз факторів навколишнього середовища, зокрема місцезнаходження користувача, час входу у систему, поведінкові характеристики тощо. Додавання біометричної аутентифікації, яка включатиме у себе розпізнавання відбитків пальців, обличчя або голосу, в залежності від того що компанія вибере для своєї системи, забезпечує додатковий рівень захисту, ускладнюючи несанкціонований доступ до системи.

Для практичної реалізації методу підвищення стійкості ЕЦП був обраний програмний пакет на основі мови програмування Python із застосуванням криптографічної бібліотеки PyCryptodome.

Верифікація підпису виконується наступним чином (рис.1): після підписання документ може бути переданий іншій стороні для перевірки, тоді система використовує публічний ключ для верифікації підпису, при цьому використовуються додаткові перевірки на цілісність даних, що дозволяє виявити модифікацію даних після підписання.

Впровадження методу включало в себе тестування можливих векторів атак на криптографічні ключі та моделювання сценаріїв компрометації даних. Одним із запропонованих способів захисту є використання апаратних модулів безпеки (HSM) [3], які забезпечують ізольоване зберігання ключів, що в подальшому унеможливлює їх витік навіть у разі компрометації серверного середовища на якому вони можуть зберігатися.

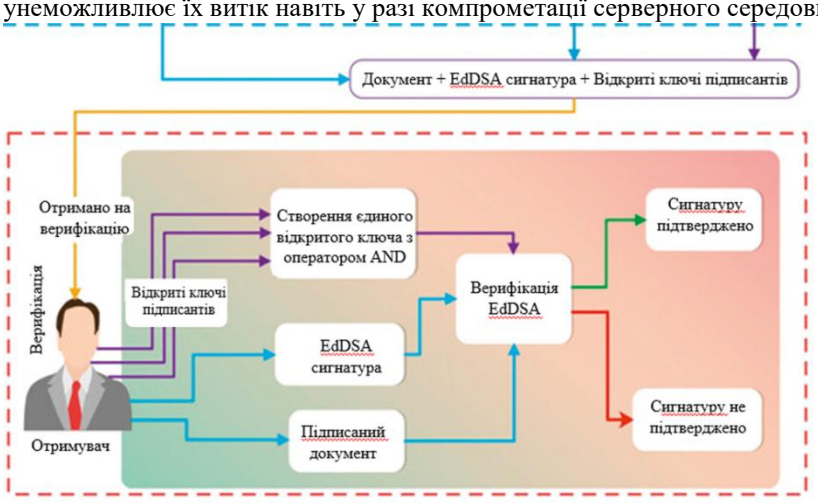

Рис.1. Процес перевірки ключів за даним методом

Відповідно запропонований метод підвищення стійкості ЕЦП складається з кількох важливих етапів: вибір нових криптографічних алгоритмів; інтеграція HSM для зберігання ключів; впровадження мультифакторної аутентифікації.

Практична цінність дослідження полягає у можливості впровадження запропонованого методу у корпоративних інформаційних системах, банківських установах та урядових структурах для підвищення рівня безпеки ЕЦП та аутентифікації користувачів. Запропонований підхід дозволяє зменшити ризики, пов’язані з компрометацією криптографічних ключів, що робить його ефективним рішенням у сфері інформаційної безпеки.

Список використаних джерел:

1. Albahadily, Hassan & Jabbar, Ismael & Altaay, Alaa & Ren, Xunhuan. (2023). Issuing Digital Signatures for Integrity and Authentication of Digital Documents. Al-Mustansiriyah Journal of Science. 34. 50-55. 10.23851/mjs.v34i3.1278.

2. Mahansaria, D., Roy, U.K. Contextual authentication of users and devices using machine learning. Computing 106, 4083–4107 (2024). https://doi.org/10.1007/s00607-024-01333-7.

3. Sommerhalder, M. (2023). Hardware Security Module. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_16