

АНАЛІЗ ТА ВПРОВАДЖЕННЯ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ФІНАНСОВИХ ОПЕРАЦІЙ

Корсакова А.В, науковий керівник Вайганг Г.О., к.т.н., доц.

У процесі цифрової трансформації фінансового сектору значно зросли обсяги електронних транзакцій, що супроводжується збільшенням кіберзагроз, спрямованих на компрометацію фінансових даних. Класичні методи захисту вже не відповідають вимогам сучасного інформаційного середовища, тому все більшого значення набуває впровадження криптографічних рішень, здатних забезпечити належний рівень безпеки та довіри до цифрових фінансових сервісів [1], [2].

Криптографія пропонує ефективні механізми захисту, які активно застосовуються в протоколах безпечного обміну (SSL/TLS), цифрових підписах, блокчейн-інфраструктурах та смарт-контрактах [3], [4]. З урахуванням динаміки розвитку криптоаналітики та потенціалом квантових технологій, забезпечення стійкості таких систем до новітніх атак набуває стратегічного значення [2]. Отже, дослідження теми криптографічного захисту фінансових операцій є вкрай актуальним, оскільки поєднує складові інформаційної безпеки, прикладного програмування та управління ризиками у цифровій економіці.

Метою дослідження є аналіз сучасних криптографічних методів захисту фінансових транзакцій та визначення ефективних напрямів їх впровадження. Завдання включають вивчення типових кіберзагроз, класифікацію алгоритмів шифрування, оцінку протоколів (SSL/TLS, HTTPS, PGP, блокчейн) та розробку рекомендацій з інтеграції захисту в IT-інфраструктуру фінансових установ.

Об'єктом дослідження є інформаційні процеси та системи, що забезпечують виконання та захист фінансових транзакцій. Предметом виступають криптографічні методи, алгоритми, протоколи й засоби, що гарантують конфіденційність, автентичність і незмінність переданих даних.

Особливу увагу приділено практичному аспекту – оцінці ефективності впровадження криптографічних механізмів у системах електронного банкінгу, платіжних сервісах, блокчейн-технологіях тощо. У результаті дослідження планується розробити рекомендації щодо вибору і застосування оптимальних криптографічних рішень для підвищення рівня інформаційної безпеки фінансових операцій [3].

Для досягнення поставленої мети дослідження передбачено аналіз актуальних кіберзагроз у сфері електронних фінансових операцій, дослідження фундаментальних принципів криптографії, класифікація основних типів алгоритмів шифрування (симетричних, асиметричних, хеш-функцій, цифрового підпису), а також оцінка ефективності захищених протоколів обміну даними, таких як SSL/TLS, HTTPS, PGP і блокчейн-рішення, що забезпечують безпечну передачу фінансової інформації.

Крім того, дослідження охоплює аналіз практичних кейсів впровадження криптографічних технологій у банківських платформах, сервісах електронної комерції та онлайн-банкінгу. На підставі узагальнення отриманих результатів буде розроблено концептуальні рекомендації щодо вибору та інтеграції криптографічних засобів у фінансову інфраструктуру. Завершальним етапом стане оцінювання запропонованих рішень з позицій надійності, швидкодії та відповідності вимогам галузевих стандартів інформаційної безпеки.

Практичне значення дослідження полягає в можливості використання його результатів для підвищення інформаційної безпеки у фінансових інформаційних системах шляхом впровадження сучасних криптографічних рішень у банківські IT-системи, платіжні платформи та політики захисту даних. Отримані напрацювання також

можуть бути корисними в освітньому та дослідницькому процесі для підготовки фахівців у сфері кібербезпеки та створення відповідного навчального забезпечення.

Рисунок 1 демонструє UML-діаграму послідовності, яка відображає процес захисту фінансової транзакції із залученням криптографічного сервісу та модуля ШІ. Взаємодія між користувачем, програмним клієнтом, системами шифрування та обробки даних дозволяє забезпечити оцінку ризику, шифрування, безпечне виконання й збереження транзакції.



Рис. 1. UML-діаграма послідовності захисту фінансової транзакції з використанням криптографії та штучного інтелекту

Такий підхід реалізує багаторівневий захист, поєднуючи аналітичні можливості штучного інтелекту з надійністю криптографічних алгоритмів, що забезпечує високу стійкість до атак і відповідність сучасним стандартам інформаційної безпеки.

Результати дослідження демонструють ефективність використання криптографічних методів у фінансових системах з урахуванням сучасних загроз. Запропоновані рішення сприяють підвищенню рівня інформаційної безпеки, що є критичним фактором для цифрової економіки та відповідності міжнародним стандартам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Плотніков В. М., Борцова Ю. В. Алгоритмізація шифрування цифрового підпису. Automation of technological and business processes, 2020. Т. 12, No 1. С. 48–54.
2. Шрамченко Б. Л. Підвищення швидкодії алгоритмів шифрування / Б. Л. Шрамченко // Мехатронні системи: інновації та інжиніринг : тези доповідей V Міжнародної науково-практичної конференції, м. Київ, 4 листопада 2021 року. – Київ : КНУТД, 2021. – С. 180-181.
3. Романюк, О.О. Програмна реалізація алгоритму шифрування RSA [Текст] / О.О. Романюк, М. П. Смаглюк; кер. С.О. Білоус // Інформатика, математика, автоматика: матеріали та програма науково-технічної конференції, м. Суми, 17- 21 квітня 2017 р. / Відп. за вип. С.І. Проценко. - Суми: СумДУ, 2017. - С. 65.
4. Гринюк С., Поліщук М. Використання технології шифрування інформації для безпечної передачі в мережі. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION. 2020. No 39. С. 122–126.

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**



**ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ
АСПЕКТИ РОЗРОБКИ
КОМП'ЮТЕРНИХ СИСТЕМ**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
*24 квітня 2025 року***

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендел

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.

Передрук матеріалів, а також використання їх будь-якій формі допускається лише з дозволу авторів