3. Pelzl J. Understanding cryptography: a textbook for students and practitioners. Springer; 2010.
4. Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A. Digital identity guidelines. National Institute of Standards and Technology; 2022 Dec 16.

Криптографічні методи захисту даних в системах електронних платежів

УДК 004.056:336.71

Людмила Бабала[1], Степан Зубик[2]

Західноукраїнський національний університет[1,2]
l.duma@wumu.edu.ua[1], *stipaha4444@gmail.com*[2]

Сучасні системи електронних платежів є важливим елементом цифрової фінансової інфраструктури, що забезпечує швидке проведення транзакцій та обмін фінансовою інформацією. Основними вимогами до таких систем є конфіденційність, цілісність, автентичність та захист від несанкціонованого доступу. Для реалізації цих вимог використовуються сучасні криптографічні алгоритми та методи інформаційної безпеки [1].

На рисунку 1 представлено UML-діаграму архітектури системи захисту інформаційних ресурсів в електронних платіжних системах. Діаграма демонструє взаємодію клієнтського інтерфейсу, модуля автентифікації, криптографічного модуля, платіжного шлюзу, системи моніторингу та аналітики шахрайських операцій. Особливу роль відіграють криптографічні алгоритми хешування, цифрового підпису та симетричного шифрування, що забезпечують конфіденційність і цілісність платіжної інформації [1, 3].

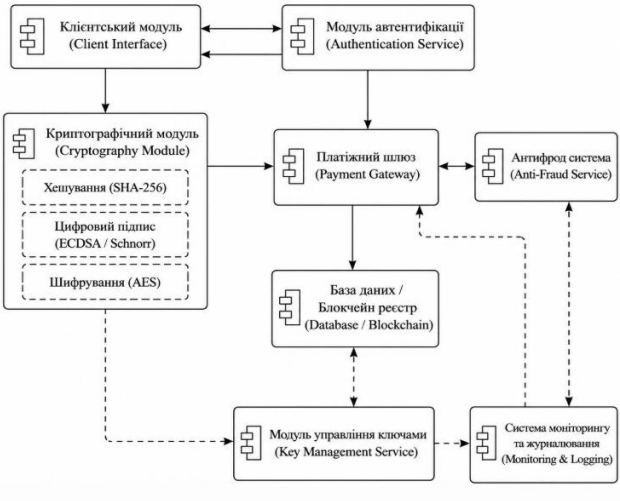

Рис. 1. Структурна UML-діаграма взаємодії криптографічних модулів та компонентів безпеки в системі електронних платежів

Одним із ключових механізмів захисту є криптографічні хеш-функції, які забезпечують контроль цілісності інформації та захист від підміни даних. У системах електронних платежів вони застосовуються для створення унікальних ідентифікаторів транзакцій, перевірки достовірності повідомлень та збереження незмінності інформації. Найбільш поширеними є алгоритми SHA-256, SHA-3 та BLAKE2, які характеризуються високою стійкістю до колізій та швидкістю обробки даних [2].

Для підтвердження автентичності та невідмовності фінансових операцій використовуються алгоритми цифрового підпису, зокрема ECDSA (Elliptic Curve Digital Signature Algorithm). Їх перевагами є висока криптостійкість, компактність ключів та швидкість обчислень. Використання цифрового підпису забезпечує перевірку справжності відправника та захист від підробки транзакцій [2, 3].

Додатковий рівень захисту реалізується через симетричне шифрування AES (Advanced Encryption Standard), яке використовується для шифрування платіжної інформації, захисту каналів зв'язку та безпечного зберігання конфіденційних даних. Використання режимів шифрування GCM і CTR дозволяє забезпечити не лише конфіденційність, а й цілісність переданих повідомлень [2].

Важливим аспектом безпеки електронних платіжних систем є комплексний підхід до захисту. Навіть найнадійніші криптографічні алгоритми можуть бути неефективними у випадку помилок конфігурації, програмних вразливостей або людського фактора. Саме тому сучасні системи електронних платежів поєднують криптографічні методи із багаторівневими механізмами кіберзахисту [1, 4].

Отже, комплексне використання хешування, цифрового підпису та симетричного шифрування дозволяє підвищити рівень безпеки інформаційних ресурсів у системах електронних платежів. Поєднання криптографічних алгоритмів із моделюванням архітектури системи сприяє підвищенню стійкості до кіберзагроз та оптимізації процесів захисту даних. Подальший розвиток цифрових технологій і квантових обчислень зумовлює необхідність удосконалення існуючих та впровадження постквантових криптографічних алгоритмів [3, 4].

1. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. З-38 Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236с.
2. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС. 2009.
3. Pelzl J. Understanding cryptography: a textbook for students and practitioners. Springer; 2010.
4. Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A. Digital identity guidelines. National Institute of Standards and Technology; 2022 Dec 16.