Пріоритет — зміцнення базових засад захисту — контроль доступу, сегментація, автоматичний патчинг, нульова довіра та виявлення аномалій мають бути негайно посилені.

Проактивна оборона з використанням ШІ — створення центрів протидії загрозам ШІ, що застосовують ті самі інструменти для захисту, ефективніше за спроби блокувати окремі моделі.

Управління ризиками та стратегічні інвестиції — кібербезпека має стати пріоритетом ради директорів; потрібні чіткі дорожні карти, збільшення фінансування і підготовка до постквантових загроз.

1. URL :https://www.bain.com/insights/claude-mythos-and-ai-cybersecurity-wake-up-call/ (дата звернення: 07.05.2026)
2. URL https://www.mindstudio.ai/blog/claude-mythos-vs-opus-4-6-cybersecurity-gap (дата звернення: 07.05.2026)
3. Bell, David. (2026). Mythos and the Question Nobody Wants to Answer.

Алгоритми забезпечення безпеки інформаційних ресурсів в системах електронних платежів

УДК 004.056:336.74

Людмила Бабала[1], Андрій Сенюк[2]

Західноукраїнський національний університет[1,2]
l.duma@wumu.edu.ua[1], *seniukandrii2003@gmail.com*[2]

Сучасний розвиток цифрових технологій сприяв активному впровадженню систем електронних платежів у фінансовій сфері. Використання інтернет-банкінгу, мобільних застосунків, цифрових гаманців та електронних платіжних платформ значно підвищує швидкість проведення фінансових операцій, однак водночас створює нові виклики у сфері забезпечення безпеки інформаційних ресурсів [1]. Особливої актуальності набуває проблема захисту конфіденційних даних користувачів, банківської інформації та фінансових транзакцій від несанкціонованого доступу, кібератак та шахрайських дій.

Системи електронних платежів є складними інформаційно-комунікаційними структурами, які об’єднують банки, платіжні сервіси, торговельні платформи та кінцевих користувачів. Через значну кількість учасників процесу та постійний обмін інформацією виникає необхідність застосування ефективних алгоритмів захисту інформаційних ресурсів [2].

Одним із базових інструментів забезпечення інформаційної безпеки електронних платежів є криптографічні алгоритми. Їх застосування спрямоване на захист конфіденційності, цілісності та автентичності інформації. Найбільш поширеним є використання симетричних і асиметричних методів шифрування. Симетричні алгоритми, зокрема AES (Advanced Encryption Standard), забезпечують швидке шифрування великих обсягів даних, що є важливим під час обробки платіжних транзакцій [3]. Асиметричні алгоритми, такі як RSA, використовуються для безпечного обміну ключами та електронного цифрового підпису [4].

Важливим напрямом забезпечення безпеки електронних платежів є використання алгоритмів багатофакторної аутентифікації (MFA). Традиційний спосіб підтвердження особи за допомогою логіна та пароля більше не гарантує належного рівня захисту, тому активно застосовуються додаткові механізми перевірки: одноразові SMS-коди, біометрична ідентифікація, підтвердження через мобільні застосунки або токени [3]. Використання багатофакторної аутентифікації дозволяє значно знизити ризик компрометації облікових записів користувачів.

Окрему роль у забезпеченні інформаційної безпеки відіграють алгоритми виявлення шахрайських операцій (Fraud Detection Systems). Такі алгоритми базуються на технологіях штучного інтелекту та машинного навчання, які аналізують поведінку користувача, географічне розташування, частоту транзакцій та інші характеристики фінансової активності [2]. У разі виявлення аномальної поведінки система автоматично блокує операцію або вимагає додаткової перевірки. Наприклад, якщо транзакція здійснюється в незвичному місці або перевищує типовий ліміт витрат, система може визначити її як потенційно небезпечну.

Суттєве значення має також використання алгоритмів моніторингу мережевого трафіку та систем виявлення вторгнень (IDS/IPS). Такі механізми дозволяють оперативно реагувати на спроби кібератак, виявляти шкідливе програмне забезпечення та запобігати витоку інформації [1]. Особливо актуальним це є в умовах поширення DDoS-атак, фішингових кампаній та використання шкідливих програм для викрадення банківських реквізитів.

Варто зазначити, що ефективність захисту електронних платежів значною мірою залежить від комплексного застосування різних алгоритмів інформаційної безпеки. Використання лише одного механізму захисту не гарантує достатнього рівня безпеки, тому сучасні платіжні системи реалізують багаторівневу архітектуру кіберзахисту, яка включає шифрування, автентифікацію, моніторинг транзакцій, резервне копіювання та постійне оновлення систем безпеки [4].

Таким чином, алгоритми забезпечення безпеки інформаційних ресурсів у системах електронних платежів є ключовим елементом стабільного функціонування цифрової фінансової інфраструктури. Застосування сучасних криптографічних методів, багатофакторної аутентифікації, алгоритмів машинного навчання для виявлення шахрайства та систем моніторингу мережевої активності дозволяє значно знизити рівень кіберризиків і підвищити довіру користувачів до електронних платіжних сервісів. Подальший розвиток технологій кібербезпеки сприятиме удосконаленню систем захисту інформаційних ресурсів та забезпеченню стійкості фінансового сектору до сучасних кіберзагроз.

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.

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].

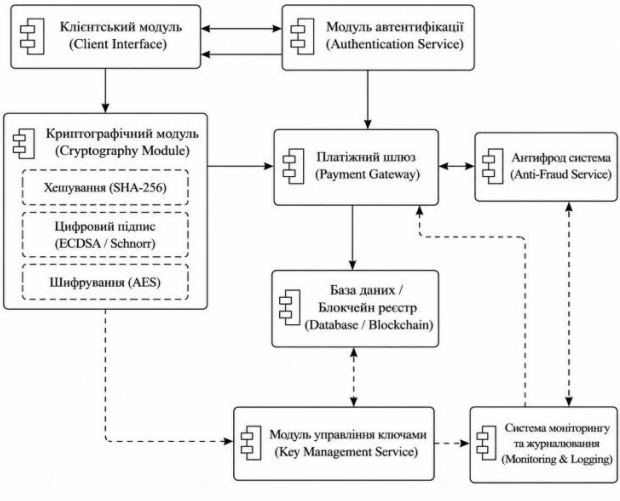

Рис. 1. Структурна UML-діаграма взаємодії криптографічних модулів та компонентів безпеки в системі електронних платежів