Of particular interest are emerging privacy-enhancing technologies (PETs) that can be deployed at the platform level: differential privacy for analytical queries, federated learning that enables training of ML models without centralising user data, homomorphic encryption for confidential computation, and zero-knowledge proofs for age or identity verification without disclosing the underlying attributes. Pilot deployments of these mechanisms by major operators (Apple, Google, Meta) demonstrate the feasibility of combining service functionality with strong privacy guarantees, although wider adoption still requires industry-level standardisation, economic incentives and clear regulatory expectations.

Conclusions. Security in social media is a complex socio-technical problem at the intersection of technical, legal and behavioural aspects, which cannot be solved by one party alone. The combination of platform-side protection mechanisms, requirements of GDPR and Law No. 2297-VI, organisational policies and conscious user behaviour substantially reduces the risks of leaks and manipulation. Further research should focus on ML models for detecting coordinated inauthentic behaviour and on adapting regulatory mechanisms to the challenges of generative AI.

1. Farooq A., Salminen J., Martin J. D., Aldous K., Jung S.-G., Jansen B. J. Exploring Social Media Privacy Concerns: A Comprehensive Survey Study Across 16 Middle Eastern and North African Countries. IEEE Access. 2024. Vol. 12. P. 147087–147105.
2. Hlavatska A., Anhelska O., Opirskyi I. Research of OSINT technology as a new threat of person deanonymisation in cyberspace. Cybersecurity: Education, Science, Technique. 2024. Vol. 1, Iss. 25. P. 19–50. (in Ukrainian)
3. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends (application date: 07.05.2026).
4. Law of Ukraine «On the Protection of Personal Data» of 01.06.2010 No. 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (application date: 07.05.2026).

## Застосування блокового шифру «Кипарис» для шифрування приватних даних у блокчейн-транзакціях

УДК 004.056.55

Марія Родінко

*Харківський національний університет імені В. Н. Каразіна, mariia.rodinko@karazin.ua*

Публічні блокчейни за своєю концепцією є прозорими – всі транзакції доступні для перегляду, що створює проблему конфіденційності для застосувань, що оперують чутливими даними. Виникає потреба в ефективному симетричному шифруванні, яке забезпечить приватність без втрати продуктивності мережі. Метою дослідження є розробка методу інтеграції перспективного постквантового блокового шифру «Кипарис» у блокчейн-

інфраструктуру для забезпечення конфіденційності даних у транзакціях із збереженням верифікованості та цілісності.

Блоковий шифр «Кипарис» [1] було розроблено з урахуванням вимог до постквантових примітивів. Перевагами алгоритму є висока швидкодія, стійкість до диференціального криптоаналізу, постквантова стійкість [2].

Запропонована схема криптографічного захисту базується на поєднанні симетричного шифрування, постквантових примітивів та децентралізованих технологій для забезпечення цілісності даних.

Нижче описані ключові етапи циклу гібридного шифрування.

1) *Генерація ключа*. Створення випадкового сесійного ключа (256/512 біт залежно від необхідного рівня стійкості) із використанням криптографічно стійкого генератора псевдовипадкових чисел.
2) *Шифрування даних алгоритмом «Кипарис»*. Використання ARX-архітектури алгоритму забезпечує високу швидкість обробки на пристроях з обмеженими ресурсами та мінімальну затримку.
3) *Інкапсуляція ключа*. Захист сесійного ключа публічним ключем отримувача за допомогою PQC-алгоритму (на базі решіток, наприклад, ML-KEM). Це гарантує стійкість до квантового криптоаналізу (алгоритм Шора).
4) *Розподілене зберігання*. Розміщення гешу шифротексту, посилання та зашифрованого сесійного ключа в блокчейні, а шифротексту – в off-chain сховищі (IPFS) для оптимізації навантаження на мережу. Отримувач, завантаживши дані з IPFS, порівнює їхній геш із записом у блокчейні.

Інтеграція «Кипарису» в архітектуру децентралізованої обробки транзакцій створює надійний рівень захисту приватних даних, дозволяючи реалізувати механізми вибіркового доступу та гарантувати конфіденційність.

1. Andrushkevych A., et al. A prospective lightweight block cipher for green IT engineering. *Green IT Engineering: Social, Business and Industrial Applications*. Cham: Springer International Publishing. – 2018. – P. 95-112.
2. Родінко, Марія Юріївна. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів : дисертація ... доктора філософії за спеціальністю 122 – комп'ютерні науки (12 – Інформаційні технології). – Харків : Харківський національний університет імені В. Н. Каразіна, 2020. – 201 с.

## Автоматизація реагування на інциденти у мультихмарних середовищах засобами SOAR-платформ: проблеми крос-хмарної інтеграції

УДК 004.056.5

Марценюк Є. В. [1]

*Національний університет «Львівська політехніка»,*
*[1]yevhenii.v.martseniuk@lpnu.ua*