рішень: автономної контейнерної платформи UNIWA на основі OpenStack та Docker [1] та платформи EMP для bootcamp-формату на 6–11 віртуальних машинах [2]. Відмінність полягає у комбінованому використанні віртуальних машин і контейнерів на базі гіпервізора рівня закладу освіти (Proxmox VE) замість хмарних платформ, що знижує бар'єри впровадження для регіональних університетів [3].

Результати апробації підтверджують працездатність запропонованої методології. Контейнеризація CTFd-сервісів і сегментація мережі firewall-правилами забезпечили повну ізоляцію вразливих сервісів від штатних навчальних середовищ протягом 24 годин роботи. Механізм знімків Proxmox VE дозволив швидко повертати середовища у вихідний стан між раундами без впливу на сусідні команди. Фактичне навантаження під час змагання (CPU до 50 %, RAM близько 90 %) залишилося нижчим за граничні показники стенду (850 одночасних HTTP-з'єднань, 1,8 Гбіт/с трафіку), що свідчить про наявний запас потужності. Розроблена методологія придатна для проведення CTF-змагань регіонального масштабу на базі кіберполігонів закладів освіти з open-source стеком віртуалізації.

1. Chouliaras N., Kantzavelou I., Maglaras L., Pantziou G., Ferrag M. A. A novel autonomous container-based platform for cybersecurity training and research. PeerJ Computer Science. 2023. Vol. 9. Article e1574. DOI: 10.7717/peerj-cs.1574.
2. Arnold D., Ford J., Saniie J. Architecture of an Efficient Environment Management Platform for Experiential Cybersecurity Education. Information. 2025. Vol. 16, No. 7. Article 604. DOI: 10.3390/info16070604.
3. Schafeitel-Tähtinen T., Lazarov W. Teaching and Learning Cybersecurity Using Capture the Flag: Effectiveness Comparison Between University Students in Finland and Czechia. Computer Applications in Engineering Education. 2025. Vol. 33, No. 5. Article e70082. DOI: 10.1002/cae.70082.

Privacy and information security in social media

UDK 004.056.5:004.738.5

Andrii Manko[1], Zhanna Babiak[2]

Ternopil Ivan Puluj National Technical University,
[1]andreymanko4@gmail.com, [2]b.janna73@gmail.com

Social media have become the primary channel for interpersonal and mass communication: according to DataReportal estimates, in 2025 they were actively used by more than 5.2 billion people — about 64 % of the world population. Modern platforms accumulate unprecedented volumes of personal data: contacts, geolocations, biometric templates (face and voice recognition), interaction history, behavioural patterns and psychometric profiles. The combination of these data with artificial intelligence tools, in particular AI-based open-data aggregation and generative models (deepfake), creates qualitatively new risks to the privacy and information security of users, organisations and the state as a whole [1, 2].

The objective of the work is to systematise current threats to privacy and information security in social media and to substantiate a complex of technical and organisational measures that mitigate these risks both at the level of the platform provider and at the level of the end user.

The relevance is driven by the rapid growth in the number and scale of incidents. According to ENISA Threat Landscape 2024, social media remain among the top three vectors for phishing and account takeover; large-scale leaks such as the 2021 Facebook incident (533 million records) and recurring compromises of the open APIs of X (Twitter), Telegram and LinkedIn demonstrate the systemic nature of the problem [3]. An additional factor in the Ukrainian context is the hybrid information operations under the conditions of the war: social media are actively used for coordinated disinformation, adversarial OSINT, profiling of military personnel from open posts and targeted phishing against the civilian population [2, 3].

The scientific novelty consists in systematising threats with regard to modern capabilities of AI-based open-data aggregation and generative synthetic content models, and in formulating a two-level «platform — user» protection model that combines technical means, regulatory requirements and behavioural practices of users [4].

As a result of the study, five main classes of threats have been identified. 1) Personal data leaks caused by attacks on platforms, open APIs and third-party applications (SQL injections, authentication vulnerabilities, cloud-storage misconfigurations). 2) Social engineering: phishing through direct messages and links, spoofing of trusted contacts, account takeover via password guessing and SIM-swap attacks. 3) Profiling and de-anonymisation through AI aggregation of open sources (OSINT) — combining data fragments from several platforms makes it possible to re-identify a person even in cases of formal anonymisation [2]. 4) Manipulative content: video and voice deepfakes, disinformation narratives, coordinated inauthentic behaviour (CIB) of botnets. 5) Disclosure of metadata and geolocation through EXIF data of photos, check-ins, messenger activity and background telemetry collection by client applications.

To mitigate the listed threats, a two-sided complex of measures is proposed. On the platform side: implementation of the «privacy by design» principle, minimisation of collected data, end-to-end message encryption (E2EE), restriction of OAuth token scopes, anomaly detection based on machine-learning models (graph neural networks, ensembles of outlier-detection algorithms), automated labelling of synthetic content with digital watermarks (in particular C2PA manifests), regular independent security audits and bug-bounty programmes. On the user side: multi-factor authentication with FIDO2 hardware keys, regular audit of third-party application permissions, restriction of public profile telemetry (private account, disabled geotags), use of different e-mail addresses for different platforms, and a critical attitude towards unverified content, especially audio and video recordings concerning sensitive topics.

At the organisational level, enterprises and public institutions should implement acceptable-use policies for social media, regular cyber-hygiene training, DLP solutions and formalised DPIA procedures for any integrations with external platforms and APIs, in line with GDPR and Law No. 2297-VI.

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-