несанкціонованого доступу, витоку даних та атак на клієнтську частину застосунку. У таких умовах важливого значення набуває використання сучасних frontend-технологій із підтримкою механізмів безпечної взаємодії користувачів із системою.

Одними з найбільш популярних інструментів для створення сучасних веб-застосунків є React.js та TailwindCSS. React.js дозволяє реалізовувати компонентний підхід до розробки інтерфейсу та забезпечує ефективне керування станом застосунку, а TailwindCSS використовується для створення адаптивного та оптимізованого інтерфейсу користувача.

Метою роботи є розробка безпечного клієнтського інтерфейсу веб-платформи для ігрової спільноти з використанням React.js та TailwindCSS, що забезпечує ефективну взаємодію користувачів із системою та підвищення рівня захисту даних.

У процесі дослідження було проаналізовано сучасні підходи до побудови frontend-інтерфейсів та визначено основні загрози безпеці клієнтської частини веб-платформи. Реалізовано клієнтський інтерфейс, який забезпечує перегляд новин, турнірів та іншого тематичного контенту, а також підтримує механізми авторизації користувачів і контроль доступу до функціоналу системи.

Для підвищення безпеки застосовано механізми захисту від XSS-атак, безпечного зберігання токенів авторизації та обмеження доступу до окремих компонентів інтерфейсу. Використання компонентної архітектури React.js забезпечило модульність системи та спростило реалізацію захищених елементів взаємодії користувача із платформою.

Отримані результати підтверджують ефективність використання сучасних frontend-технологій для створення безпечних веб-платформ. Використання React.js та TailwindCSS дозволяє забезпечити адаптивність інтерфейсу, покращити продуктивність системи та підвищити рівень захисту клієнтської частини веб-застосунку.

1. React Documentation [Електронний ресурс]. – Режим доступу: https://react.dev/.
2. Tailwind CSS Documentation [Електронний ресурс]. – Режим доступу: https://tailwindcss.com/docs/.
3. Banks A., Porcello E. Learning React. – O'Reilly Media, 2020.

Full cycle of responding to cyber incidents in the public sector

UDC 004.056 Iryna Tegubenko[1], Viktor Kotetunov[2]

State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, [1]wr.irttri@gmail.com [2]v.kotetunov@gmail.com

An important factor in ensuring cyber protection of Ukraine in modern conditions is the availability of civil servants, primarily of higher categories, comprehensive knowledge of the current state of cybersecurity, trends of changes in the industry, and understanding of the continuity of the cyclical process of responding to cyber incidents.

The reality of the current moment is characterized by the acceleration of the evolution of cyber security, in particular due to the influence of artificial intelligence technologies [1], an increase in the speed of computing processes, a rapid increase in the complexity and volume of data that must be processed and taken into account in the processes of analyzing the state of cyber security, the transition to a risk-oriented approach to cyber security, the correlation of domestic approaches with the international practices of CISA [2], NIST [3], MITER ATT&CK[4], etc.

Each of the participants in public administration should be familiar with the processes of organizing the full cycle of response to cyber incidents, its main components, properties, and resources, and understand their place, functions, and acquire the necessary competencies. The complete cyber incident response cycle consists of several interrelated modules, namely: the preparation, the detection and analysis, the deterrence, the elimination, the recovery, and the analysis of the effectiveness of cyber incident response measures. In fact, it is a cyclical process, the main one of which is the preparation stage, in terms of the amount of resources, time, and qualifications required. The stage is performed almost continuously. If immediate cyber incident response actions begin at the time a cyber incident is initiated, the outcome for the institution will be known to be negative.

1. Hilpisch Y., Ali M.G., Jasim A.K., Abdulrahman S.A.R., Abu-AlShaeer M.J., Almansoori K.W.N., Tregubenko I. Strategic Technological Integration and National Industrial Resilience: Assessing AI-Driven Efficiency Across Critical Sectors. (2026), 2855 CCIS, pp. 507 - 522, DOI: 10.1007/978-3-032-17023-1_30
2. Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. URL: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks (application date 07.05.2026).
3. NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (application date 07.05.2026).
4. Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK). URL: https://attack.mitre.org (application date 07.05.2026).

Розробка алгоритму виявлення ШІ-згенерованих зображень на основі машинного навчання

УДК 621.395.7 (043.2)

Фляк Владислав

Національний університет "Одеська політехніка",10328099@stud.op.edu.ua

Сьогодні цифрові технології радикально змінили спосіб сприйняття інформації. Фотографії та відео вже не є надійним доказом реальності події, оскільки штучний інтелект здатний створювати повністю синтетичний контент, який важко відрізнити від справжнього. ШІ-згенеровані зображення стали масовим явищем у соціальних мережах, рекламі, медіа та навіть судовій практиці. Це призводить до кризи довіри до візуальної інформації та створює