УДК 004.056

***Целуєв В.О., здобувач,***
***Савіцький Р.С., аспірант, ст. викладач***
*Державний університет «Житомирська політехніка»*

## МЕТОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ КОРИСТУВАЧІВ У ГЕЙМЕРСЬКИХ СОЦІАЛЬНИХ МЕРЕЖАХ

Стрімкий розвиток ігрових соціальних мереж супроводжується накопиченням значних обсягів чутливих персональних даних користувачів, таких як ігрова статистика, платіжна інформація, геолокаційні дані, записи голосового та текстового чату. За даними звітів з кібербезпеки, ігрова індустрія входить до трійки найбільш атакованих секторів, що свідчить про критичну необхідність комплексного підходу до захисту персональних даних на таких платформах.

Аналіз існуючих ігрових платформ, таких як Steam, Discord, Battle.net, виявив типові вразливості, а саме зберігання паролів у незашифрованому вигляді, відсутність обмежень на кількість спроб входу, недостатній контроль доступу до API-ендпоінтів. На основі проведеного аналізу загроз за методологією STRIDE розроблено багаторівневу модель захисту персональних даних користувачів соціальної мережі для геймерів [1].

Перший рівень захисту реалізує шифрування даних у стані спокою за алгоритмом AES-256 та транспортне шифрування TLS 1.3 для всіх з'єднань між клієнтом і сервером. Паролі користувачів зберігаються виключно у вигляді хешів, отриманих алгоритмом bcrypt із коефіцієнтом складності 12, що унеможливлює їх відновлення навіть у разі витоку бази даних [2].

Другий рівень забезпечує багатофакторну автентифікацію, яка реалізована як підтримка TOTP-кодів через застосунки Google Authenticator та Authy, апаратних ключів стандарту FIDO2/WebAuthn, а також адаптивна автентифікація з аналізом поведінкових патернів користувача. Система автоматично блокує обліковий запис після п'яти невдалих спроб входу та надсилає сповіщення власнику [3].

Третій рівень включає контроль доступу на основі ролей (RBAC) та атрибутів (ABAC) при зверненні мікросервісів до бази даних. Реалізація принцип мінімальних привілеїв надає перевагу в контролі. Кожен сервіс має доступ лише до тих таблиць і полів, які необхідні для виконання його функцій. Персональні дані псевдонімізуються перед передачею до аналітичних підсистем відповідно до вимог GDPR.

Для виявлення підозрілої активності впроваджено систему моніторингу на базі ELK Stack (Elasticsearch, Logstash, Kibana) з набором правил кореляції подій. Журнали аудиту всіх операцій із персональними даними зберігаються у незмінному сховищі протягом 90 днів. Час реакції системи на виявлену аномалію не перевищує 3 секунди, після чого автоматично ініціюється процедура блокування підозрілої сесії.

Тестування на проникнення варто проводити за методологією OWASP Testing Guide v4.2, щоб підтвердити відсутність критичних вразливостей класів SQL Injection, XSS та IDOR у реалізованій системі. Навантажувальне тестування показує стабільну роботу модуля автентифікації при одночасній обробці 5 000 запитів на секунду без деградації часу відповіді.

Окремої уваги заслуговує організація безпечного зберігання медіаконтенту користувачів, таких як аватари, знімки екрану та ігрові кліпи. Усі завантажені файли проходять перевірку сигнатур для виявлення замаскованих виконуваних файлів, зберігаються в ізольованому об'єктному сховищі S3-сумісного типу та доступні виключно через підписані тимчасові URL-посилання з терміном дії 15 хвилин, що унеможливлює несанкціонований прямий доступ до медіафайлів.

Запропонована багаторівнева модель захисту відповідає вимогам Загального регламенту захисту даних ЄС та Закону України «Про захист персональних даних» [4, 5]. Практична цінність роботи полягає у можливості адаптації розробленої архітектури для широкого класу соціальних платформ із великою кількістю користувачів. Подальші дослідження спрямовані на впровадження технологій виявлення аномалій на основі машинного навчання для проактивного захисту облікових записів від компрометації.

**Список використаних джерел:**

1. OWASP Top Ten 2023. Open Web Application Security Project. – URL: https://owasp.org/Top10.

2. Stallings W. Cryptography and Network Security. – Pearson, 2022. – 816 p.

3. Howard M., LeBlanc D. Writing Secure Code. – Microsoft Press, 2003. – 800 p.

4. Regulation (EU) 2016/679 (General Data Protection Regulation). – Official Journal of the EU, 2016.

5. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.