Кібербезпека в індустрії розробки відеоігор: загрози для індустрії

Андрій Ілюшка
студент кафедри комп'ютерних наук,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: iliushkaay@krok.edu.ua
Микита Фешенко
асистент кафедри комп'ютерних наук,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: feshchenkom@krok.edu.ua,
ORCID: 0009-0002-6290-4323
Віра Ткаченко
к.ф.-м.н., доцент, доцент кафедри інформаційного менеджменту,
математики та статистики,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: tkachenkov@krok.edu.ua,
ORCID: 0000-0001-6064-5474

Актуальність теми зумовлена тим, що відеоігри перетворилися на одну з ключових сфер цифрової економіки, де збіг високої комерційної вартості інтелектуальної власності, відкритості інфраструктури та глобального характеру взаємодії створює унікальні можливості для кібератак. Для розуміння, кібербезпека – це комплекс процесів, рекомендацій і технологічних рішень, які допомагають захистити важливі системи, дані й мережу від цифрових атак [1]. З огляду на це, перехід до аналізу реальних загроз є необхідним кроком для формування системного бачення безпеки в індустрії, де атаки вже давно виходять за межі класичних сценаріїв і охоплюють гібридні, багаторівневі та технологічно складні моделі.

Об'єктом дослідження виступають процеси, інфраструктура та цифрові активи, задіяні у виробництві відеоігор, включно з інтелектуальною власністю, серверною інфраструктурою та поведінковими даними користувачів.

Предметом даного дослідження є сучасні кіберзагрози, що безпосередньо впливають на індустрію розробки відеоігор як високотехнологічний та високоризиковий сегмент цифрової економіки.

Метою дослідження є попередній опис, класифікація та аналітичне узагальнення найбільш значущих загроз, які формують сучасне поле ризику для компаній-розробників відеоігор.

Однією з найбільш масштабних загроз для розробників є програми-вимагачі, зокрема моделі так званого подвійного шантажу, коли зловмисники не лише шифрують дані, а й викрадають критичні масиви інформації, включно з вихідними кодами та збірками, після чого погрожують їх оприлюдненням. Саме ця тенденція особливо характерна для індустрії розробки відеоігор, де вартість незавершених продуктів і кодових баз значно перевищує традиційні корпоративні ризики через неможливість замінити викрадену інтелектуальну власність. Ключові аспекти такої загрози ґрунтовно описано у рекомендаціях

CISA, де підкреслюється швидка еволюція тактик подвійного шантажу та її вплив на цифрові компанії різного масштабу [2].

Не менш небезпечним явищем є атаки на ланцюг постачання. У розробці відеоігор широко використовуються сторонні модулі, бібліотеки, пакети, плагіни, а також складні інтегровані середовища збірки. Компрометація будь-якого з таких елементів дає змогу зловмисникам інтегрувати шкідливий код безпосередньо в середовище розробки [3]. Додатковим вектором ризику є компрометація CI/CD, коли зловмисники отримують контроль над процесом автоматизованої збірки. Як свідчать звіти Unit42, доступ до пайплайнів відкриває можливість підміни збірок, викрадення секретів та створення бекдорів у фінальних продуктах, що робить цю загрозу однією з найнебезпечніших для ігрової галузі, де більшість релізів використовують автоматизований випуск оновлень [4].

Інсайдерські загрози становлять окремий комплекс ризиків, особливо в індустрії з високою кадровою мобільністю та численними підрядниками. Витік вихідних кодів, збірок, асетів або внутрішньої документації значною мірою пов'язаний саме з людським фактором, що підтверджують узагальнені дослідження CISA, які вказують на зростання ролі інсайдерів у структурі кіберінцидентів у різних галузях [5]. До цього типу загроз належить і промислове шпигунство, спрямоване на викрадення пропрієтарних технологій або планів монетизації, що має особливо високі наслідки для студій, які працюють над унікальними рушіями чи інноваційними механіками.

Фішинг і соціальна інженерія, включно з використанням deepfake-технологій, посідають чільне місце серед сучасних загроз для галузі. Розробники часто ведуть активну публічну діяльність, а їхня комунікація зі спільнотою створює сприятливе середовище для атаки через імітацію рекрутингу, керівництва або колег. У публікаціях NSA та FBI зафіксовано стрімке поширення голосових та deepfake-відео, застосованих у фішингових кампаніях, які здатні переконати жертв виконувати критичні дії, що робить такі методи особливо ефективними в середовищах із віддаленою роботою та високим робочим навантаженням [6].

Ігрові сервери, що працюють у режимі високої доступності, стають мішенню DDoS-атак, які безпосередньо впливають на бізнес-результати видавців та студій. Аналітика Cloudflare підтверджує, що геймінг систематично входить до числа найбільш атакованих секторів, а характер трафіку UDP та низькі допуски до затримки ускладнюють застосування класичних механізмів захисту, перетворюючи DDoS на стратегічну загрозу для серверної інфраструктури ігрових продуктів [7].

Ризики телеметрії та персональних даних гравців становлять окрему категорію загроз. Збір поведінкових, технічних та соціальних даних створює значні можливості для профілювання, а витік таких даних призводить до серйозних юридичних та фінансових наслідків. Наукові дослідження у сфері цифрової приватності підтверджують, що ігрові платформи збирають великі масиви даних, які при компрометації можуть бути використані для соціальної інженерії, фінансових атак або стороннього аналізу без згоди користувачів,

що суттєво посилює потребу в якісних механізмах захисту та відповідності нормативам GDPR і COPPA [8].

Висновки. Загрози, виявлені у процесі аналізу, формують багатовимірне поле ризику. Таким чином, сучасна система безпеки має враховувати характер цих загроз, їхню взаємозалежність та еволюційну динаміку, оскільки комплексність проблеми свідчить про те, що захист ігрової індустрії потребує системного оновлювання та міждисциплінарного підходу.

Ключові слова: кібербезпека, індустрія відеоігор, витік данних, DDoS-атаки.

Список використаних джерел

1. Microsoft. (2024). What is cybersecurity? Отримано з https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity (дата звернення 24.11.2025).
2. The Cybersecurity and Infrastructure Security Agency (CISA). (2023). #StopRansomware Guide. Отримано з https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (дата звернення 26.11.2025).
3. Sonatype. (2020). The SolarWinds software supply chain attack: how developers can protect applications. Отримано з https://www.sonatype.com/blog/software-supply-chain-attacks-solarwind-how-developers-fortify-apps (дата звернення 26.11.2025).
4. Palo Alto Networks. (2024). Anatomy of a cloud supply pipeline attack. Отримано з https://www.paloaltonetworks.com/cyberpedia/anatomy-ci-cd-pipeline-attack (дата звернення 26.11.2025).
5. The Cybersecurity and Infrastructure Security Agency (CISA). (2020). Insider threat mitigation guide. Отримано з https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf (дата звернення 27.11.2025).
6. The Cybersecurity and Infrastructure Security Agency (CISA). (2023). Contextualizing deepfake threats to organizations. Отримано з https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats (дата звернення 27.11.2025).
7. Cloudflare, Inc. (2025). Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report. Отримано з https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/ (дата звернення 27.11.2025).
8. SSRN. (2021). Surveilling the gamers: privacy impacts of the video game industry. Отримано з https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881279 (дата звернення 27.11.2025).