КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.928
УДК 004.056.5:004.942

**Полотай Орест Іванович**
кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID 0000-0003-4593-8601
*orest.polotaj@gmail.com*

**Брич Тарас Богданович**
кандидат технічних наук, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID 0000-0001-6853-1981
*taras_brych@hotmail.com*

**Ткаченко Артур Мар'янович**
викладач кафедри безпеки інформаційних технологій
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID ID *0009-0009-6830-4741*
*tkachenko.am14@gmail.com*

**Дітковський Максим Михайлович**
здобувач вищої освіти 4 курсу групи КБ-410, кафедра безпеки інформаційних технологій
Національний університет Львівська Політехніка, Львів, Україна
*maksym.ditkovskyi.kb.2022@lpnu.ua*

**Гуменюк Максим Романович**
здобувач вищої освіти 3 курсу групи КБ-32, кафедра управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
*maxhumeniuk321@gmail.com*

# ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СУЧАСНИХ МЕРЕЖЕВИХ ІГРАХ

**Анотація.** У статті розглянуто проблематику інформаційної безпеки в сучасних мережевих іграх, які в умовах цифровізації стали не лише інструментом розваг, але й важливою частиною соціальної взаємодії та комунікацій. Акцент зроблено на комплексному аналізі основних кіберзагроз, які постають перед користувачами та розробниками ігрових сервісів. Зокрема, детально досліджено поширені атаки на облікові записи, фішингові схеми, використання ботів і шкідливого програмного забезпечення, а також реалізацію масових DDoS-атак, спрямованих на порушення доступності ігрових серверів. Особливу увагу приділено соціально-інженерним методам впливу, що поєднують технічні та психологічні аспекти впливу на гравців. Важливою складовою дослідження стала побудова моделі загроз інформаційної безпеки, яка систематизує типи атак, умови їх виникнення, рівень збитків, об'єкти порушення (конфіденційність, цілісність, доступність) та типові мережеві порти, що використовуються для реалізації загроз. Запропонована класифікація дозволяє виділити найбільш небезпечні напрямки впливу на ігрові системи та формує основу для подальшої розробки захисних механізмів. Показано, що значна частина атак стає можливою через уразливості операційної системи Windows, яка є найпоширенішою серед геймерів. Серед критичних проблем виділено експлойти драйверів, вразливості мережевих служб (SMB, RDP, RPC), недоліки файлової системи, загрози від несвоєчасного оновлення системи та використання zero-day експлойтів. У роботі окремо підкреслюється важливість дослідження вразливостей ОС Windows у контексті забезпечення безпеки мережевих ігор. Візуалізація ключових векторів атак у вигляді інфографіки наочно демонструє багаторівневий характер ризиків і вказує на необхідність розробки комплексних методів захисту. Додатково наведено результати аналізу останніх наукових публікацій і звітів індустрії, які підтверджують зростання кількості атак на гравців і розробників та підкреслюють недостатність традиційних

засобів безпеки. Практичним внеском дослідження стала концепція створення інструмента на мові Python для виявлення мережевих атак у режимі реального часу. Запропоновано використання бібліотек для аналізу трафіку (Scapy, Socket, PyShark) та алгоритмів виявлення аномалій у поведінці мережевих пакетів. Це відкриває перспективи для створення ефективних захисних рішень, адаптованих під специфіку онлайн-ігор, а також закладає основу для подальшої інтеграції інтелектуальних систем на базі машинного навчання. У висновках наголошено, що інформаційна безпека в мережевих іграх є багатокомпонентною проблемою, яка охоплює як технічні, так і соціальні аспекти. Визначено необхідність комплексного підходу, що включає модернізацію протоколів безпеки, регулярне оновлення операційних систем, впровадження античіт-технологій, систем виявлення вторгнень, а також формування культури безпечної поведінки серед гравців. Перспективи подальших досліджень вбачаються у розширенні функціоналу розробленого програмного інструмента, застосуванні методів штучного інтелекту для прогнозування атак, а також у стандартизації підходів до оцінки безпеки ігрових екосистем. Таким чином, результати дослідження мають як наукове, так і практичне значення: вони систематизують існуючі загрози, виявляють ключові слабкі місця у безпеці сучасних ігрових середовищ та пропонують прикладні рішення, що сприятимуть підвищенню рівня захищеності користувачів і довіри до цифрових розважальних платформ.

**Ключові слова:** інформаційна безпека; онлайн-ігри; мережеві загрози; вразливості Windows; DDoS-атаки; фішинг; захист даних; Python-інструменти моніторингу.

## ВСТУП

У сучасному інформаційному суспільстві мережеві ігри посідають значне місце серед цифрових сервісів, які активно використовуються мільйонами користувачів по всьому світу. Вони перестали бути лише засобом розваг та перетворилися на соціально-культурний феномен, що об’єднує різні вікові та професійні групи. Паралельно з розвитком індустрії онлайн-ігор зростає й кількість загроз, пов’язаних із захистом персональних даних, фінансових транзакцій та цілісності ігрових акаунтів.

Особливістю сучасних багатокористувацьких ігор є їхня висока інтеграція з інтернет-сервісами, хмарними платформами та соціальними мережами. Це створює нові канали поширення кіберзагроз і підвищує ризики витоку конфіденційної інформації. Гравці дедалі частіше стають мішенню для шахрайських схем, фішингових атак, використання шкідливого програмного забезпечення.

Таким чином, питання інформаційної безпеки в мережевих іграх набуває особливої актуальності. Недостатній рівень захисту не лише створює ризик фінансових втрат, але й підриває довіру до розробників, платформ та спільнот гравців. У цих умовах виникає необхідність системного дослідження загроз та методів їх подолання.

**Постановка проблеми.** Проблема інформаційної безпеки в сучасних мережевих іграх полягає у зростаючій кількості кіберзагроз, які спрямовані на порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Традиційні методи захисту, що застосовуються розробниками, не завжди здатні ефективно протидіяти новим формам атак. Це обумовлює потребу у створенні комплексних підходів до забезпечення безпеки.

Серед основних загроз варто відзначити фішинг, соціальну інженерію, крадіжку акаунтів, злом внутрішньоігрових економік, використання ботів і чітів. Крім того, уразливими залишаються канали зв’язку між клієнтом та сервером, що може призвести до перехоплення даних чи підміни інформації.

Додатковим ускладнюючим чинником є масштабованість та динамічність ігрових систем. У багатокористувацьких онлайн-іграх (MMORPG, MOBA, шутерах тощо)

одночасно взаємодіють тисячі гравців, що створює значний простір для маніпуляцій. Це вимагає від розробників використання адаптивних методів моніторингу та захисту.

Таким чином, проблема полягає не лише в наявності технічних загроз, але й у комплексному характері безпеки, яка охоплює технологічні, організаційні та соціальні аспекти функціонування мережевих ігор.

У межах цієї статті планується розглянути такі аспекти:

- огляд інформаційних загроз у мережевих іграх;
- вразливості операційних систем сімейства Windows у процесі гри;
- мережевий аналіз і протоколи безпеки;
- основні методи та засоби захисту;
- опис прототипу розробленого програмного інструмента для виявлення мережевих атак;
- рекомендації та практичні висновки.

**Аналіз останніх досліджень і публікацій.** У сучасній літературі помітна чітка концентрація на декількох взаємопов'язаних напрямках: зростання інцидентів із захопленням акаунтів (account takeover, ATO), збільшення DDoS-атак проти ігрових сервісів та еволюція підпільного ринку «читів», що застосовують складні техніки, включно з kernel-рівневими рішеннями. Аналітика продуктових досліджень і звіти індустрії свідчать про помітне зростання атак на гравців і платформу в цілому, що підсилює економічні та репутаційні ризики для розробників і сервіс-провайдерів [1].

Академічні дослідження останніх років (кілька робіт 2023–2025 рр.) зосереджуються на двох основних групах підходів: розробка алгоритмів виявлення шахрайства й читів (аналітика поведінки, машинне навчання для виявлення аномалій у траєкторіях ігроків, статеві моделі тощо) та дослідження інженерних практик розробників щодо інтеграції безпеки у життєвий цикл гри [11]. Якісні інтерв'ю з розробниками показують підвищену усвідомленість проблеми, але – одночасно – брак ресурсів та стандартизованих практик для інтегрованого захисту [2].

У напрямку мережевих загроз і DDoS-атак опубліковані звіти індустрії показують різке зростання частоти й потужності атак, а також появу спеціалізованих «DDoS-for-hire» сервісів, що робить ігрові хости уразливішими, особливо під час турнірів і пікових хвиль трафіку. Практичні дослідження та технічні репорти підкреслюють необхідність комбінованих рішень: мережеві фільтри, CDN/трафік-абсорбція, а також адаптивні алгоритми виявлення аномалій у трафіку [4].

Що стосується вразливостей операційних систем і локальних клієнтів, сучасні публікації звертають увагу на дві проблемні області: зловживання привілеями та експлуатація уразливостей драйверів (особливо коли анти-чит системи також працюють на kernel-рівні, що створює нові ризики), та ризики від сторонніх модифікацій (моди, чіти, «трейнери»), які найчастіше поширюються через соціні інженерні схеми і шкідливі інсталятори. Ці роботи наголошують на конфлікті між потребою глибокого моніторингу (для виявлення читів) і загальними принципами безпеки ОС – архітектурні рішення мають мінімізувати довіру до стороннього коду і зводити до мінімуму права доступу [5].

Методологічні підходи в останніх публікаціях включають: використання машинного навчання для класифікації аномалій у поведінці гравців; евристичні та сигнатурні методи для ідентифікації відомих зразків читів; побудову симуляторів трафіку для стрес-тестування захисних механізмів; а також дослідження застосування криптографічних протоколів (DTLS/TLS, підписів повідомлень) для захисту комунікацій. Водночас відзначається брак відкритих репозиторіїв даних (annotated gameplay / network captures), що ускладнює реплікацію результатів і порівняння методів.

Попри помітні досягнення в алгоритмах виявлення шахрайства та мережевих захисних механізмах, у літературі бракує комплексних робіт, які поєднують: (a) глибокий аналіз вразливостей ОС при реальному запуску ігрового клієнта, (b) метричні підходи до оцінки ефективності анти-чит рішень без порушення приватності, та (c) практичних реальних інструментів для виявлення мережевих атак у режимі реального часу з відкритим кодом для реплікації результатів.

**Мета статті.** Метою дослідження є аналіз основних загроз інформаційній безпеці в сучасних мережевих іграх та обґрунтування ефективних методів захисту, що дозволять підвищити рівень безпеки користувачів та зменшити ризики кіберзлочинності у сфері онлайн-ігор, та запропонувати прототип розробленого програмного інструмента для виявлення мережевих атак.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Серед різноманіття сучасних масових багатокористувацьких онлайн-ігор (MMO) особливе місце займають проєкти військово-тематичного спрямування, які пропонують гравцям можливість керування бронетехнікою різних історичних періодів. Такі ігри поєднують елементи симуляції, стратегії та змагального шутера, формуючи окремий сегмент кіберспортивної та розважальної індустрії.

World of Tanks – одна з найвідоміших ігор жанру, розроблена компанією Wargaming.net. Вона репрезентує класичну модель MMO-бойовика, де ключовим елементом є командні бої між гравцями на історичних зразках бронетехніки XX століття. Гра відзначається гнучкою системою розвитку, численними варіантами модифікацій та сильною кіберспортивною складовою. Її мобільна адаптація (World of Tanks Blitz) та консольні версії розширили аудиторію, а новий проєкт World of Tanks: Heat орієнтований на поєднання танкових боїв із динамікою hero-шутерів.

War Thunder, створена Gaijin Entertainment, вирізняється підвищеним рівнем реалістичності. Вона пропонує керування не лише танками, але й літаками та кораблями. Особливу увагу приділено фізичній моделі бою, балістиці та деталізації ураження броні. Цей проєкт приваблює гравців, які віддають перевагу симуляторним механікам.

Armored Warfare представляє альтернативний підхід до жанру. Вона орієнтована на сучасну бронетехніку та пропонує як PvP-битви, так і кооперативні PvE-місії. Поєднання класичного геймплею з елементами сценарних кампаній робить її конкурентоспроможною серед аналогічних ігор.

Enlisted поєднує історичну достовірність та багатокористувацький формат. Гравець керує взводом солдатів, де танки виступають однією зі складових геймплею поряд із піхотою та авіацією. Завдяки цьому реалізується комплексна модель бойових дій часів Другої світової війни.

Call of War: World War II представляє стратегічний напрям MMO-ігор. Вона дає змогу керувати не окремою бойовою одиницею, а цілою армією та економічною інфраструктурою, що створює умови для глобальної взаємодії гравців у режимі реального часу.

До легших за структурою, але популярних онлайн-проєктів належать Diep.io, де гравець керує умовним 2D-танком у просторі з абстрактними цілями, та Tanki Online, який відзначається простотою доступу, динамічністю і змагальною природою. Ці ігри зберігають популярність завдяки низьким вимогам до ресурсів та можливості швидкої взаємодії у браузері.

BZFlag вирізняється як класичний приклад гри з відкритим кодом. Вона має тривалу історію розвитку та підтримується спільнотою ентузіастів, що робить її важливим об'єктом для дослідження феномену open-source у геймінгу.

Modern Tanks: War Tank Games є прикладом аркадного підходу до танкових шутерів. Гра орієнтована на динаміку та візуальні ефекти, що робить її привабливою для широкої аудиторії, однак вона меншою мірою претендує на реалізм.

В таблиці 1 показано найбільш популярні онлайн-ігри.

*Таблиця 1*

**Сучасні онлайн-ігри**

| Назва гри | Платформи | Особливості |
|---|---|---|
| World of Tanks | ПК, консолі, мобільні | Класика MMO-танків |
| World of Tanks Blitz / Modern Armor | Мобільні / консолі | Мобільні/консольні версії WoT |
| World of Tanks: Heat | ПК, консолі (PS5, XSX/S), Steam Deck | Hero-shooter у танковому сеттингу |
| War Thunder | ПК, консолі | Реалістичний симулятор |
| Armored Warfare | ПК | Сучасні танки + PvE |
| Enlisted | ПК | Історичні кампанії WWII |
| Call of War: WWII | Браузер | Глобальна стратегія/MMO |
| Diep.io | Браузер / мобільні | Легка .io-гра |
| BZFlag | ПК | Open-source 3D FPS-танки |
| Tanki Online | Браузер | Кастомізація, PvP, івенти |
| Modern Tanks (Steam) | ПК (Steam) | Аркадний топ-down танковий шутер |

Зважаючи на зростаючу кількість інцидентів, пов'язаних із крадіжкою облікових записів, поширенням шахрайських схем, використанням шкідливого програмного забезпечення та здійсненням DDoS-атак проти ігрових сервісів, проблема інформаційної безпеки в онлайн-іграх набуває критичного значення. Вразливості операційних систем, недосконаліть захисних протоколів та активне використання соціальної інженерії свідчать про багатовимірний характер загроз, що охоплюють як технічні, так і поведінкові аспекти взаємодії користувачів. У цих умовах дослідження механізмів виявлення та протидії загрозам, а також розробка практичних інструментів для підвищення безпеки гравців постає як нагальна наукова й прикладна задача.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Побудуємо модель загроз інформаційної безпеки, які можуть виникати під час гри.

*Таблиця 2*

**Модель загроз**

| Тип загрози | Коли виникає | Рівень збитків | Що порушує | Типові порти, через які може виникати загроза |
|---|---|---|---|---|
| Крадіжка акаунтів | При зломі облікових записів або використанні слабких паролів | Високий | Конфіденційність, цілісність | HTTPS (443), API-порти платформ |

| | | | | |
|---|---|---|---|---|
| DDoS-атака | Під час пікових ігрових сесій або змагань | Високий | Доступність | UDP/TCP (27015–27050, 3074, 8080, 443) |
| Використання ботів | У процесі гри для отримання переваги чи шахрайських дій | Середній | Цілісність ігрового процесу | Ті ж порти, що й ігрові клієнти |
| SQL-ін’єкції | При недостатньому захисті баз даних ігрових платформ | Високий | Конфіденційність, цілісність | TCP (1433 – MS SQL, 3306 – MySQL) |
| Man-in-the-Middle | Під час передачі даних між клієнтом та сервером без належного шифрування | Високий | Конфіденційність, цілісність | HTTP (80), нестабільні TCP/UDP з’єднання |
| Віруси/трояни | При встановленні сторонніх модифікацій, "читів", піратських клієнтів | Середній – високий | Конфіденційність, цілісність, доступність | Залежить від ПЗ, часто 445 (SMB), 135 |
| Зловживання ОС | Використання вразливостей драйверів чи модулів під час роботи гри | Високий | Цілісність системи, конфіденційність | Локальні служби, системні порти ОС |
| Соціальна інженерія | При спілкуванні між гравцями чи через форуми/чати | Середній | Конфіденційність | Не залежить від конкретного порту |

Аналіз моделі загроз інформаційної безпеки в онлайн-іграх показує, що найбільш критичними є атаки, спрямовані на порушення конфіденційності та цілісності даних гравців, а також на забезпечення доступності ігрових сервісів через DDoS-атаки та зловживання вразливостями мережевих протоколів. Особливу небезпеку становлять загрози, які реалізуються через вразливості операційної системи, оскільки саме Windows є найбільш поширеною платформою серед гравців і часто виступає ціллю для шкідливого програмного забезпечення, експлойтів драйверів та несанкціонованого доступу до системних ресурсів. Це підкреслює необхідність глибокого дослідження вразливостей ОС Windows, адже вони створюють фундаментальні умови для реалізації багатьох із перелічених загроз і визначають рівень загальної безпеки онлайн-ігор.

На рис. 1 представлено основні операційної системи сімейства Windows під час онлайн ігор.


*Рис. 1. Основні вразливості операційної системи сімейства Windows під час онлайн ігор*

Цей рисунок відображає модель основних вразливостей операційної системи Windows, структурованих за ключовими зонами ризику. У центрі розташовано логотип

Windows, що символізує базову платформу, навколо якої згруповані категорії можливих атак.

У блоці "Ядро ОС" зазначено критичні загрози, пов'язані з експлойтами драйверів, привілейованим виконанням коду та переповненням буферів, що безпосередньо загрожують стабільності всієї системи. Мережеві служби охоплюють уразливості популярних протоколів, таких як SMB (порт 445), RDP (порт 3389) та RPC/DNS, які є частими мішенями для віддалених атак і поширення шкідливого ПЗ.

Користувацьке середовище відображає ризики, пов'язані з людським фактором: фішингові атаки через UAC, підроблені діалогові вікна, запуск шкідливих файлів та використання сторонніх модифікацій («читів»). У блоці "Файлова система та пам'ять" зосереджені проблеми з доступом до системних директорій, керуванням правами користувачів та витоком даних із оперативної пам'яті. Завершує схему блок "Оновлення та патчі", який підкреслює ризики несвоєчасного оновлення системи, що залишає користувачів вразливими до zero-day експлойтів.

Таким чином, рисунок 1 наочно демонструє багаторівневий характер загроз для Windows та підкреслює необхідність їх системного аналізу з метою розробки ефективних механізмів захисту, особливо у сфері онлайн-ігор, де ця операційна система домінує.

Онлайн-ігри функціонують на основі клієнт-серверної або peer-to-peer архітектури, що передбачає активне використання мережевих портів для обміну даними в режимі реального часу. Кожен ігровий клієнт встановлює мережеве з'єднання з ігровим сервером або іншими клієнтами, використовуючи певний діапазон портів (наприклад, TCP/UDP-порти у межах 27000–28000 для ігор на платформах Steam). Саме ці порти можуть стати вразливою точкою для зловмисників.

На рис. 2 показано основні вектори атак через мережеві порти.


*Рис. 2. Основні вектори атак через мережеві порти під час онлайн ігор*

Серед основних векторів атак варто виділити:

DoS/DDoS-атаки (Denial of Service / Distributed Denial of Service).

Зловмисник спрямовує надмірний обсяг трафіку на відкриті порти ігрового клієнта або сервера, перевантажуючи канал чи обчислювальні ресурси. Це призводить до затримок, розриву з'єднання та недоступності гри для легітимних користувачів.

Port Scanning (сканування портів).

Здійснюючи масове сканування, атакувальник може визначити, які порти відкриті під час ігрової сесії. Виявлені порти використовуються для подальших експлойтів, наприклад, спрямованих на служби, що працюють у фоновому режимі.

Packet Injection (ін'єкція пакетів).

Якщо мережеві порти недостатньо захищені, можливо здійснити підміну або ін'єкцію шкідливих UDP/TCP-пакетів. Це може призвести до зміни параметрів гри,

отримання несправедливої переваги або навіть до краху клієнта.

Exploitation of UDP Amplification.

Більшість онлайн-ігор активно використовують протокол UDP для швидкої передачі даних. Через відкриті порти гравців можливо здійснити UDP-ампліфікаційні атаки, коли невеликий запит генерує непропорційно великий обсяг відповіді, що посилює DDoS-навантаження.

Man-in-the-Middle (MitM).

У випадку відсутності шифрування трафіку (особливо у старіших іграх) зловмисник може перехоплювати пакети, що проходять через відкриті порти. Це дає можливість відстежувати дії гравця, підмінювати інформацію чи красти облікові дані.

Remote Code Execution через вразливості портів.

У разі наявності недоліків у реалізації ігрового протоколу або серверного програмного забезпечення, відкритий порт може використовуватися для виконання довільного коду на комп'ютері жертви.

*Приклад практичного сценарію*

Гравець під час сесії у World of Tanks чи War Thunder підтримує з'єднання через визначений UDP-порт. Атакувальник сканує цей порт та спрямовує на нього потік з підробленими пакетами, імітуючи запити від сервера. У результаті гравець отримує «затримки» (lag) або повне відключення від сесії. При масштабуванні така атака може паралізувати роботу цілого ігрового кластера.

У процесі гри в багатокористувацькі онлайн-проєкти комп'ютерна система піддається ризику як через безпосередню мережеву взаємодію, так і через уразливості операційного середовища. Для зниження ймовірності атак та збереження конфіденційності даних варто застосовувати сучасні протоколи і стандарти безпеки.

Представимо основні мережеві протоколи, та додаткові заходи безпеки які допоможуть захиститися під час онлайн гри (таблиця 3).

*Таблиця 3*

**Мережеві протоколи та заходи безпеки**

| | |
|---|---|
| **Захист мережевої взаємодії** | |
| TLS (Transport Layer Security) | Використовується для шифрування трафіку між клієнтом та сервером, що унеможливлює перехоплення облікових даних та маніпуляції з ігровими пакетами. У сучасних ігрових сервісах переважно застосовується TLS 1.3, який забезпечує високу швидкість і стійкість до криптоаналітичних атак. |
| DTLS (Datagram TLS) | Розроблений для захисту UDP-трафіку, який часто використовується в онлайн-іграх для обміну даними у реальному часі. Дозволяє шифрувати пакети без втрати продуктивності. |
| IPsec (Internet Protocol Security) | Забезпечує автентифікацію і шифрування на мережевому рівні. Доцільний для корпоративних або турнірних середовищ, де потрібен гарантований захист каналів зв'язку. |
| SSH (Secure Shell) | Використовується адміністраторами серверів для безпечного керування ігровою інфраструктурою. Хоча сам гравець не працює безпосередньо через SSH, цей протокол важливий для захисту серверної частини. |
| **Захист облікових даних і доступу** | |
| OAuth 2.0 та OpenID Connect. | Використовуються в системах автентифікації ігрових платформ (наприклад, Steam, Epic Games Store), забезпечуючи безпечну авторизацію через сторонні сервіси |
| Мультифакторна автентифікація (MFA). | Реалізується через одноразові паролі (OTP), апаратні токени або мобільні додатки (Google Authenticator, Microsoft Authenticator). Дозволяє знизити ризик компрометації акаунта навіть при витоку пароля |

| | |
|---|---|
| **Захист операційної системи під час гри** | |
| SELinux / AppArmor (Linux), Windows Defender Application Control (Windows) | Системи примусового контролю доступу, які обмежують права виконання програм, включно з іграми та їхніми модулями. Це знижує ризик запуску шкідливих модифікацій (cheat-програм, троянів). |
| Sandboxing та Virtualization | Використання вбудованих засобів ізоляції процесів (наприклад, Windows Sandbox чи Docker) дозволяє запускати ігрові клієнти в ізольованому середовищі, мінімізуючи вплив потенційно небезпечного коду на основну ОС |
| Регулярні оновлення (Patch Management) | Автоматичне застосування оновлень операційної системи, драйверів і антивірусного ПЗ є критично важливим для закриття відомих вразливостей |
| **Додаткові засоби безпеки** | |
| VPN (Virtual Private Network) | Використовується для захисту ігрового трафіку від прослуховування та для протидії DDoS-атакам, особливо у випадку професійних кіберспортивних змагань |
| Антивірусні системи з поведінковим аналізом | Дозволяють виявляти нові типи шкідливих програм, які можуть проникати під виглядом модифікацій чи сторонніх утиліт до гри |

Отже, захищеність даних та стабільність операційної системи під час онлайн-ігор досягається завдяки комплексному підходу: використанню криптографічних протоколів (TLS, DTLS, IPsec), сучасних механізмів автентифікації (OAuth, MFA), систем ізоляції та контролю доступу (SELinux, Sandbox), а також регулярному оновленню програмного забезпечення. Поєднання цих методів забезпечує надійну протидію як мережевим атакам, так і локальним загрозам.

З огляду на вищесказане було розроблено прототип програмного продукту на мові Python, який виявляє мережеву атаку під час онлайн гри. Головне вікно програми показано на рис. 3.

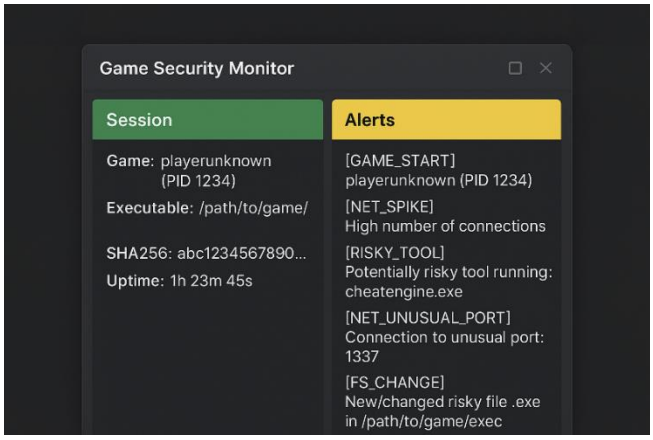


*Рис. 3. Стартовевікно програми*

На рис. 3 показана візуалізація (макет вікна) розробленого програмного забезпечення Game Security Monitor, яке ми побудували на основі твого коду.

У вікні є дві панелі:

- Session (ліва панель, зелена шапка) – показує деталі про гру:
- назва та PID процесу,
- шлях до виконуваного файлу,
- SHA256-хеш,
- час роботи.

1. Alers (права панель, жовта шапка) – виводить останні події безпеки, які система виявила:

- запуск гри,
- різкий стрибок підключень,
- виявлення підозрілих інструментів (наприклад, CheatEngine),
- підключення до нетипових портів,
- створення чи зміну ризикованих файлів.

Запропоноване програмне забезпечення, це свого роду онлайн-монітор реального часу, який виконує набір певних функцій:

- відстежує запуск/зупинку гри (за іменами типу l2.exe, lineageii.exe тощо);
- логіює шлях і SHA-256 хеш виконуваного файлу (сигналить, якщо зміниться);
- моніторить мережеві з'єднання процесу гри й попереджає про підозрілі порти/сплески;
- дивиться зміни у файловій системі в папці гри (нові .exe/.dll/.bat/.ps1 і т.ін.);
- попереджає, якщо запущені ризикові інструменти (Cheat Engine, sniffer'и, дебагери);
- веде JSONL-лог з автоповоротом та показує живу консольну панель.

Для того, щоб запустити даний монітор в операційній системі Windows, рекомендується запустити термінал від імені Адміністратора та виконати такі дії:

встановити Python 3.10+;

в консолі запустити;

*pip install psutil watchdog rich;*

додати шлях до папки з грою:

*set GSM_GAME_DIR=C:\Games\LineageII;*

запусти файл

*python game_security_monitor.py.*

На рисунку 4 показано блок-схему алгоритму роботи запропонованого онлайн-монітору.

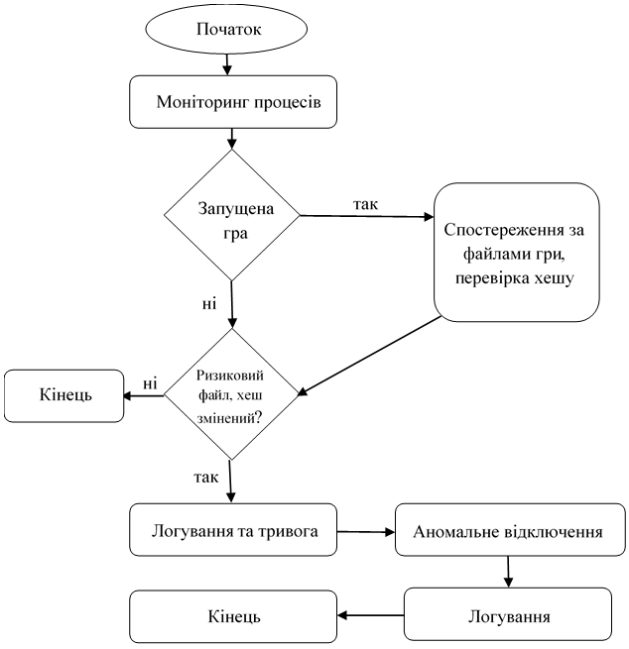


*Рис. 4. Блок-схема роботи програмного продукту*

Алгоритм роботи програмного продукту полягає в безперервному відстеженні активності комп'ютера під час запуску та функціонування ігор. На початку система активує модуль моніторингу процесів, який аналізує запущені програми з метою виявлення ідентифікації гри. Якщо гра не запущена, моніторинг продовжується у фоновому режимі, очікуючи появи відповідного процесу. У випадку, коли гра визначена як активна, додатково запускається спостереження за її файлами, що дозволяє контролювати зміни у директоріях та перевіряти нові чи модифіковані елементи на наявність ризикових розширень, таких як .exe, .dll, .bat чи скриптові файли. У разі виявлення потенційно небезпечного файлу формується відповідне повідомлення, яке заноситься до журналу подій. Паралельно система аналізує мережеву активність, відслідковуючи кількість та характер з'єднань. При виявленні аномалій, наприклад, підключень до нетипових портів або різкого зростання кількості конекцій, події також логуються для подальшого аналізу. Таким чином, програмний продукт забезпечує цілісний контроль за процесами гри, змінами у файловій системі та мережевою взаємодією, формуючи звіти про всі підозрілі або ризикові ситуації.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження підтвердило, що сучасні мережеві ігри є високоризиковим середовищем з точки зору інформаційної безпеки. У процесі аналізу було визначено основні загрози, серед яких провідне місце займають фішинг, крадіжка акаунтів, DDoS-атаки, використання шкідливого програмного забезпечення та експлуатація вразливостей операційної системи Windows. Розроблена модель загроз дозволила систематизувати їх за ключовими параметрами – момент виникнення, рівень збитків, об'єкт порушення та використовувані мережеві порти. Це надало можливість не лише класифікувати потенційні небезпеки, але й виокремити найбільш критичні напрями для подальшого захисту.

Окремо підкреслено значення вразливостей ОС Windows, яка залишається домінуючою платформою для онлайн-ігор і часто виступає головною ціллю для кіберзлочинців. Виявлені уразливості ядра, мережевих служб, файлової системи та механізмів оновлення створюють передумови для реалізації більшості атак, що підтверджує необхідність їх системного вивчення. Практична розробка програмного засобу на Python для моніторингу мережевого трафіку у режимі реального часу стала першим кроком у напрямку створення прикладних рішень, здатних виявляти підозрілу активність і своєчасно реагувати на загрози.

Перспективи подальших досліджень полягають у кількох напрямках. По-перше, доцільним є розширення алгоритмів аналізу мережевого трафіку за рахунок методів машинного навчання та глибоких нейронних мереж, що підвищить точність виявлення аномалій. По-друге, важливим завданням є створення комплексної системи оцінки ризиків, яка враховуватиме не лише технічні, але й соціальні аспекти безпеки гравців. По-третє, перспективним є формування відкритих репозиторіїв даних для тестування й верифікації запропонованих методів захисту, що сприятиме стандартизації підходів у галузі. Нарешті, особливу увагу слід приділити інтеграції розроблених захисних рішень у реальні ігрові екосистеми, що дозволить забезпечити їхню практичну ефективність та масштабованість.

Таким чином, результати дослідження мають як теоретичне, так і прикладне значення, а подальша робота в цьому напрямі сприятиме підвищенню рівня безпеки онлайн-ігор та зміцненню довіри користувачів до цифрових розважальних платформ.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kaspersky. (2024, July 23). *30 percent more young gamers targeted by cybercriminals in H1 2024 vs. H2 2023*. https://www.kaspersky.com/about/press-releases/30-percent-more-young-gamers-targeted-by-cybercriminals-in-h1-2024-vs-h2-2023
2. *Advancements in cheating detection algorithms in FPS games*. (2025). In *Proceedings of SPIE 13562, Applications of Machine Learning*. https://doi.org/10.1117/12.3061748
3. Damasevicius, R., Venckauskas, A., Grigaliunas, S., Toldinas, J., Morkevicius, N., Aleliunas, T., & Smuikys, P. (2020). LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics, 9*(5), 800. https://doi.org/10.3390/electronics9050800
4. Corero. (n.d.). *How DDoS attacks disrupt gaming*. https://www.corero.com/how-ddos-attacks-disrupt-gaming
5. Newman, L. H. (2021, April 8). *Inside the multimillion-dollar gray market for video game cheats*. *WIRED*. https://www.wired.com/story/inside-the-multimillion-dollar-grey-market-for-video-game-cheats/
6. Kanode, C. M., & Haddad, H. M. (2009). Software engineering challenges in game development. In *Sixth International Conference on Information Technology: New Generations* (pp. 260–265). IEEE. https://doi.org/10.1109/ITNG.2009.194
7. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data, 7*(1), 105. https://doi.org/10.1186/s40537-020-00373-4
8. Moreira, A. V. M., Filho, V. V., & Ramalho, G. (2014). Understanding mobile game success: A study of features related to acquisition, retention and monetization. In *Proceedings of SBGames 2014*.
9. Murphy-Hill, E., Zimmermann, T., & Nagappan, N. (2014). Cowboys, ankle sprains, and keepers of quality: How is video game development different from software development? In *Proceedings of the 36th International Conference on Software Engineering* (pp. 1–11). ACM. https://doi.org/10.1145/2568225.2568227
10. Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 130. https://doi.org/10.1186/s13638-016-0623-9
11. Klostermeyer, P., Amft, S., Höltervennhof, S., Krause, A., Busch, N., & Fahl, S. (2024). Skipping the security side quests: A qualitative study on security practices and challenges in game development. https://saschafahl.de/static/paper/gamedevs2024.pdf
12. Shushura, O. M., Asieieva, L. A., Nedashkivskiy, O. L., Havrylko, Y. V., Moroz, Y. O., Smailova, S. S., & Sarsembayev, M. (2022). Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 12*(3), 64–68. https://doi.org/10.35784/iapgos.3033
13. Завада, А. А., Самчишин, О. В., & Охрімчук, В. В. (2012). Аналіз сучасних систем виявлення атак і запобігання вторгненням. *Інформаційні системи. Збірник наукових праць ЖВІНАУ, 6*(12), 97–106.
14. Лук'яненко, Т. Ю., Поночовний, П. М., & Легомінова, С. В. (2022). Методика виявлення мережевих вторгнень і ознак комп'ютерних атак на основі емпіричного підходу. *Сучасний захист інформації, 2*(50), 15–21.
15. Толюпа, С., Плющ, О. Г., & Пархоменко, І. І. (2020). Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах. *Кібербезпека: освіта, наука, техніка, 2*(10), 169–181.
16. Чичкарьов, Є., Зінченко, О., Бондарчук, А., & Асєєва, Л. (2023). Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки. *Кібербезпека: освіта, наука, техніка, 1*(21), 234–251.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

**Orest Polotai**
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0003-4593-8601
*orest.polotaj@gmail.com*

**Taras Brych**
Candidate of Technical Sciences,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0001-6853-1981
*taras_brych@hotmail.com*

**Arthur Tkachenko**
Lecturer of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID *0009-0009-6830-4741*
*tkachenko.am14@gmail.com*

**Maksym `Ditkovskyi**
4th year higher education student, group KB-410,
Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
*maksym.ditkovskyi.kb.2022@lpnu.ua*

**Maksym Gumenuk**
3th year higher education student, group KB-32,
Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
*maxhumeniuk321@gmail.com*

# INFORMATION THREATS AND METHODS OF ENSURING SECURITY IN MODERN ONLINE GAMES

**Abstract.** The article examines the issues of information security in modern online games, which in the context of digitalization have become not only a tool for entertainment, but also an important part of social interaction and communications. The emphasis is on a comprehensive analysis of the main cyber threats that users and developers of gaming services face. In particular, widespread attacks on accounts, phishing schemes, the use of bots and malicious software, as well as the implementation of massive DDoS attacks aimed at disrupting the availability of game servers, were studied in detail. Particular attention is paid to social engineering methods of influence that combine technical and psychological aspects of influencing players. An important component of the study was the construction of a model of information security threats that systematizes the types of attacks, the conditions for their occurrence, the level of damage, objects of violation (confidentiality, integrity, availability) and typical network ports used to implement threats. The proposed classification allows us to identify the most dangerous areas of influence on gaming systems and forms the basis for further development of protective mechanisms. It is shown that a significant part of attacks becomes possible due to vulnerabilities of the Windows operating system, which is the most common among gamers. Among the critical problems, driver exploits, vulnerabilities of network services (SMB, RDP, RPC), file system shortcomings, threats from untimely system updates and the use of zero-day exploits are highlighted. The work separately emphasizes the importance of studying Windows OS vulnerabilities in the context of ensuring the security of network games. Visualization of key attack vectors in the form of infographics clearly demonstrates the multi-level nature of risks and indicates the need to develop comprehensive protection methods. Additionally, the results of the analysis of the latest scientific publications and industry reports are presented, which confirm the growth in the number of attacks on players and developers and emphasize the inadequacy of traditional security tools. The practical contribution of the study was

the concept of creating a tool in the Python language for detecting network attacks in real time. The use of libraries for traffic analysis (Scapy, Socket, PyShark) and algorithms for detecting anomalies in the behavior of network packets is proposed. This opens up prospects for creating effective protective solutions adapted to the specifics of online games, and also lays the foundation for further integration of intelligent systems based on machine learning. The conclusions emphasize that information security in online games is a multi-component problem that covers both technical and social aspects. The need for a comprehensive approach is identified, including the modernization of security protocols, regular updates of operating systems, the implementation of anti-cheat technologies, intrusion detection systems, and the formation of a culture of safe behavior among players. Prospects for further research are seen in expanding the functionality of the developed software tool, the application of artificial intelligence methods for predicting attacks, and the standardization of approaches to assessing the security of gaming ecosystems. Thus, the research results have both scientific and practical significance: they systematize existing threats, identify key weaknesses in the security of modern gaming environments, and offer applied solutions that will help increase the level of user security and trust in digital entertainment platforms.

**Keywords:** information security; online games; network threats; Windows vulnerabilities; DDoS attacks; phishing; data protection; Python monitoring tools.

## REFERENCES

1. Kaspersky. (2024, July 23). *30 percent more young gamers targeted by cybercriminals in H1 2024 vs. H2 2023*. https://www.kaspersky.com/about/press-releases/30-percent-more-young-gamers-targeted-by-cybercriminals-in-h1-2024-vs-h2-2023
2. *Advancements in cheating detection algorithms in FPS games*. (2025). In *Proceedings of SPIE 13562, Applications of Machine Learning*. https://doi.org/10.1117/12.3061748
3. Damasevicius, R., Venckauskas, A., Grigaliunas, S., Toldinas, J., Morkevicius, N., Aleliunas, T., & Smuikys, P. (2020). LITNET-2020: An annotated real-world network flow dataset for network intrusion detection. *Electronics, 9*(5), 800. https://doi.org/10.3390/electronics9050800
4. Corero. (n.d.). *How DDoS attacks disrupt gaming*. https://www.corero.com/how-ddos-attacks-disrupt-gaming
5. Newman, L. H. (2021, April 8). *Inside the multimillion-dollar gray market for video game cheats*. *WIRED*. https://www.wired.com/story/inside-the-multimillion-dollar-grey-market-for-video-game-cheats/
6. Kanode, C. M., & Haddad, H. M. (2009). Software engineering challenges in game development. In *Sixth International Conference on Information Technology: New Generations* (pp. 260–265). IEEE. https://doi.org/10.1109/ITNG.2009.194
7. Kasongo, S. M., & Sun, Y. (2020). Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset. *Journal of Big Data, 7*(1), 105. https://doi.org/10.1186/s40537-020-00373-4
8. Moreira, A. V. M., Filho, V. V., & Ramalho, G. (2014). Understanding mobile game success: A study of features related to acquisition, retention and monetization. In *Proceedings of SBGames 2014*.
9. Murphy-Hill, E., Zimmermann, T., & Nagappan, N. (2014). Cowboys, ankle sprains, and keepers of quality: How is video game development different from software development? In *Proceedings of the 36th International Conference on Software Engineering* (pp. 1–11). ACM. https://doi.org/10.1145/2568225.2568227
10. Osanaiye, O., Cai, H., Choo, K.-K. R., Dehghantanha, A., Xu, Z., & Dlodlo, M. (2016). Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 130. https://doi.org/10.1186/s13638-016-0623-9
11. Klostermeyer, P., Amft, S., Höltervennhof, S., Krause, A., Busch, N., & Fahl, S. (2024). *Skipping the security side quests: A qualitative study on security practices and challenges in game development*. https://saschafahl.de/static/paper/gamedevs2024.pdf
12. Shushura, O. M., Asieieva, L. A., Nedashkivskiy, O. L., Havrylko, Y. V., Moroz, Y. O., Smailova, S. S., & Sarsembayev, M. (2022). Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 12*(3), 64–68. https://doi.org/10.35784/iapgos.3033

13. Zavada, A. A., Samchyshyn, O. V., & Okhrimchuk, V. V. (2012). Analysis of modern attack detection and intrusion prevention systems. *Information Systems. Collection of Scientific Papers of ZhVINAU*, *6*(12), 97–106.
14. Lukyanenko, T. Yu., Ponochovnyi, P. M., & Legominova, S. V. (2022). Methodology for detecting network intrusions and signs of computer attacks based on an empirical approach. *Modern Information Protection, 2*(50), 15–21.
15. Tolyupa, S., Plyushch, O. G., & Parkhomenko, I. I. (2020). Building attack detection systems in information networks based on neural network structures. *Cybersecurity: Education, Science, Technology*, *2*(10), 169–181.
16. Chichkarev, E., Zinchenko, O., Bondarchuk, A., & Aseeva, L. (2023). Feature selection method for intrusion detection system using ensemble approach and fuzzy logic. *Cybersecurity: Education, Science, Technology*, *1*(21), 234–251.