НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

14. Create a Role Hierarchy. Trailhead, Salesforce. URL: https://trailhead.salesforce.com/content/learn/modules/data_security/data_security_roles
15. Cybersecurity Challenges in Cloud-based CRM. SSRN Working Paper, 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5005031
16. Best Practices for Protecting Your CRM Data. National Cybersecurity Alliance (StaySafeOnline), 2025. URL: https://staysafeonline.org/articles/best-practices-for-protecting-your-crm-data

Ключові слова: CRM, персональні дані, конфіденційність, доступ на основі ролей, правила шерингу, шифрування, моніторинг подій, Privacy Center, Hyperforce, резидентність даних.
Keywords: CRM, personal data, confidentiality, role-based access, sharing rules, encryption, event monitoring, Privacy Center, Hyperforce, data residency.

ЗАХИСТ ІГРОВИХ РЕСУРСІВ У СУЧАСНИХ ВІДЕОІГРАХ: КОНЦЕПЦІЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ В ГРІ «HONEY & MOLD»

Дяченко Аріна

студентка 4 курсу факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія»

Соколов Артем

доктор технічних наук, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»

Сфера відеоігор є однією з найдинамічніших і фінансово потужних галузей цифрової індустрії: щороку ігровий ринок залучає мільярдні інвестиції та забезпечує значні прибутки розробникам, видавцям і сервісним платформам. В умовах такої конкуренції успіх ігрового продукту значною мірою залежить від ефективності механізмів захисту внутрішніх ресурсів [1, 2]. Порушення цілісності ігрових даних, втручання у збереження, маніпуляції з внутрішньою економікою чи обхід механік прогресу можуть не лише руйнувати баланс гри, але й завдавати прямих фінансових збитків.

Сучасні відеоігри давно вийшли за межі традиційних розваг і перетворилися на складні програмні системи, в яких поєднуються елементи кібербезпеки, управління даними, штучного інтелекту та мережевої інфраструктури. Тому захист внутрішніх ігрових ресурсів стає критично важливим завданням і для великих студій, і для розробників. Особливо актуальним це є у проєктах, де економічний баланс визначає динаміку геймплею й безпосередньо впливає на користувацький досвід.

Метою цієї роботи є проєктування системи безпеки ресурсів гри «Honey & Mold».

У даній роботі розглянуто концепцію та реалізацію ігрового проєкту «Honey & Mold» – стратегії з елементами виживання, в якій гравець керує бджолиною маткою, що має відновити свій улей, збираючи ресурси, формуючи черги робочих бджіл і створюючи спеціальні костюми для подолання перешкод. Гра поєднує механіки управління чергами завдань, систему життєвих циклів робочих бджіл, крафт та наративні елементи у вигляді лже-артефактів, що розкривають приховану історію світу.

У процесі розробки ігрового проєкту особливого значення набуває визначення ресурсів, що є критичними для ігрової економіки та, відповідно, становлять підвищений ризик несанкціонованої модифікації. У грі «Honey & Mold» таким ресурсом є мед, який виступає базовою внутрішньоігровою валютою, впливає на прогрес, баланс і доступність ігрових механік. Тому захист цілісності даного ресурсу потребує окремого технічного забезпечення.

Найпоширенішими загрозами для подібних ресурсів виступають:

– пряме редагування локальних значень у пам’яті під час виконання гри;

– маніпуляції файлами збережень;

– модифікація кінцевих станів за допомогою утиліт на кшталт Cheat Engine;

– застосування спеціальних «тренерів», що змінюють логіку виконання окремих функцій, перехоплюють виклики API або підміняють параметри гри під час роботи.

Для запобігання таким атакам у проєкті застосовується кілька взаємодоповнювальних механізмів:

1. Центральним елементом захисту є система локальних збережень на основі SQLite із криптографічним шифруванням полів та вбудованим хеш-значенням, що підписується за допомогою секретного ключа. Під час кожного завантаження даних гра здійснює перевірку відповідності хеш-значення, підписаного ключем, що зберігається у програмі [3]; у разі виявлення відмінностей дані розглядаються як модифіковані, а система або відновлює коректний стан з резервної копії, або ініціює захисну реакцію, наприклад, сповіщення користувача чи блокування підозрілих змін.

2. Щоб унеможливити підроблення лише підсумкових значень, використовується подвійний журнал транзакцій із незворотною моделлю дописування, а також механізм відновлення action-log, який дозволяє відтворити повну історію операцій та перевірити достовірність фінального стану через детерміністичне виконання подій. Такий підхід суттєво ускладнює втручання в економіку гри навіть при використанні інструментів на кшталт Cheat Engine, оскільки зміна одного лише числового значення не відповідає транзакційній історії та неминуче призводить до виявлення невідповідності.

3. Для протидії тренерам, що працюють через ін'єкцію коду або підміну функцій, застосовуються перевірки цілісності виконуваного коду, контроль сигнатур основних DLL, періодична валідація критичних функцій з використанням обфускації та випадкових структур даних, а також часткове перенесення логіки перевірки ресурсів у приховані внутрішні модулі, що динамічно генеруються під час виконання.

Комплексне застосування цих механізмів, посилене телеметричним моніторингом через Steamworks API, забезпечує надійний захист ключових ігрових ресурсів і підтримує стабільність внутрішньоігрової економіки навіть за умов активних спроб маніпуляції з боку користувачів.

Запропонована система захисту ігрових ресурсів відеогри «Honey & Mold» демонструє ефективність поєднання криптографічних методів, журналювання транзакцій та перевірок цілісності коду для запобігання несанкціонованим змінам локальних даних та обходу внутрішньоігрової логіки. Водночас запропоновані підходи є масштабованими та можуть бути адаптовані для інших ігрових проєктів із різними жанрами та моделями економіки, забезпечуючи стабільність внутрішньоігрових систем і захист критичних ресурсів.

Перспективними напрямами подальших досліджень є проведення практичного тестування ефективності описаних механізмів на різних платформах, оцінка стійкості проти сучасних інструментів для модифікації пам'яті, інтеграція методів машинного навчання для автоматичного виявлення потенційних атак та аномалій у поведінці користувачів, а також розробка спеціалізованих криптографічних алгоритмів, адаптованих для роботи з іграми. Таке поєднання теоретичних та практичних підходів дозволяє підвищити надійність ігрових систем та формує основу для подальшого розвитку досліджень у сфері кібербезпеки відеоігор.

Список використаної літератури:

1. Huang J. et al. Improved Public-Key Searchable Encryption Scheme for Cloud-Based Responsible Gaming Systems. Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC). IEEE, 2024. P. 1-3.
2. Lukas M., Tomicic I., Bernik A. Anticheat system based on reinforcement learning agents in unity. Information. 2022. Vol. 13, No. 4. P. 173.
3. Mohammed Q. A. A. S., Joudah M., Mohammed H. A survey on digital signature schemes. AIP Conference Proceedings. AIP Publishing LLC, 2024. Vol. 3232. No. 1. P. 020057.

Ключові слова: захист даних, відеоігри, шифрування, хешування, локальна база даних, кібербезпека.
Keywords: data protection, video games, encryption, hashing, local database, cybersecurity.

ЗМІСТ