УДК 004.056

Палій О.М.

АНАЛІЗ ЗАГРОЗ КІБЕРБЕЗПЕЦІ КОМП'ЮТЕРНИХ ІГОР ЖАНРУ RPG

Анотація

У роботі проаналізовано відомі загрози кібербезпеці у сучасних іграх. Проведено їх аналіз на основі реальних фактів атак, визначено вразливості та запропоновано основний засіб протидії.

Ключові слова: *загрози комп'ютерним іграм, гра, RPG, блокчейн*

Abstract

The paper analyzes the known threats to cybersecurity in modern games. Their analysis is based on the real facts of the attacks, vulnerabilities are identified and the main means of counteraction is proposed.

Key words: *security threats, game, RPG, blockchain*

Вступ

На сьогодні комп'ютерні ігри користуються попитом у всіх вікових груп. Встановлючи гру на свій комп'ютер, користувач надає їй частковий доступ до своєї операційної системи, піддаючи себе загрозам зі сторони зловмисників, якщо розробники не спроектують працюючий модуль захисту [1]. Метою цієї роботи є покращити захист гри від загроз кібербезпеці. Для цього потрібно розв'язати такі задачі: проаналізувати загрози; виділити вразливості, на які спрямовані ці загрози; запропонувати профілактичні задачі для уникнення загроз

Результати дослідження

Для кращого аналізу загроз комп'ютерним іграм потрібно розглянути можливі атаки та вразливості, визначити об'єкти та модулі на які вони спрямовані. Аналіз джерел інформації [2-5] показав, що об'єктами атак можуть бути:

- програмний код ігрових серверів;
- доступність серверів;
- цілісність трафіку;
- програмний код клієнтської частини гри.

Якщо програмне забезпечення на ігровому сервері було зламано, комп'ютери, які підключаються до нього, також можуть зазнати взлому. Будь-яка гра з мережевим підключенням несе певний ризик для безпеки особистих даних гравця. Використовуючи вразливості, зловмисник може віддалено керувати комп'ютером гравця і використовувати його для атаки на інші комп'ютери. Прикладом такої атаки є отримання доступу до комп'ютера користувача через гру «Age of Conan» [3]. Використання вразливого коду дозволило хакерам читати файли з комп'ютерів гравця та віддалено виключати інші запущені застосунки [3]. Тобто, було порушено основні принципи кібербезпеки: конфіденційність, цілісність та доступність [2].

Атакуючи ігрові сервери, зловмисник може зробити його недосяжним для гравців, і в результаті цього користувачі не зможуть підключитись і отримати доступ до свого аккаунта, дані від якого зберігаються на сервері. Тобто, ставиться під питання їх

доступність, прикладом реалізації такої атаки є систематична відмова роботи серверів компанії EA [4].

Зловмисник з метою отримання ігрових привілегій, може підмінити значення, які відправляются на сервер. Тобто, підмінити наприклад кількість отриманої ігрової валюти, якщо вона розраховується на стороні клієнта. Прикладом використання такої вразливості, є гра GTA Online, у якій за допомогою казино і зміни суми реального виграшу у пакеті, який відправляється на сервер, є можливість швидкого збагачення [5].

Розглянувши можливі та найбільш поширені загрози, доцільно одразу запропонувати рішення для їх уникнення. Найбільш правильним буде використання технології «блокчейн» [6]. Основною перевагою є стабільність, тобто, підтверджені дані навряд чи будуть скасовані, а це означає, що як тільки дані були зареєстровані в блокчейні, їх надзвичайно важко видалити або змінити.

Висновок

Після проведенння аналізу можливих загроз та вразливостей, прикладів їх використання зловмисником, можна зробити висновок, що основні проблеми сучасних ігор відносяться до неправильного або некорректного налаштування серверів та їх захисту. Тому запропоновано рішення використання технології блокчейну, яка полегшить роботу в більшості напрямків розробки сучасної гри.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Bier, Vicki & Azaiez, Naceur. (2009). Game Theoretic Risk Analysis of Security Threats. 10.1007/978-0-387-87767-9.
2. Grzegorz Milka Anatomy of Account Takeover URL: https://www.usenix.org/conference/enigma2018/presentation/milka/ (дата звернення: 22.05.2022).
3. Eric J. Hayes Playing it Safe: Avoiding Online Gaming Risks URL: https://www.cisa.gov/uscert/sites/default/files/publications/gaming.pdf (дата звернення: 22.05.2022)
4. Yadullah Abidi Are EA Servers down right now? URL: https://candid.technology/ea-servers/ (дата звернення: 22.05.2022)
5. Jagrit Arora GTA V Online Money Glitch URL: https://techyjungle.com/gta-5-online-money-glitch/ (дата звернення: 22.05.2022)
6. Blockchain Advantages and Disadvantages URL: https://academy.binance.com/en/articles/positives-and-negatives-of-blockchain (дата звернення: 22.05.2022)

Палій Олексій Миколайович *– студент групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: alexey.paliy1337@gmail.com*

Науковий керівник: ***Баришев Юрій Володимирович*** *– кандидат технічних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет*

Olexii Palii *- student of group 1BS-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail:* alexey.paliy1337@gmail.com

Supervisor: ***Yurii Baryshev*** *— PhD (Eng), Associated Professor of the Department of Information Protection, Faculty of Information Technologies and Computer Engineering. Vinnytsia National Technical University.*