https://doi.org/10.28925/2664-2069.2024.11

ESPORTS AND CYBERSECURITY: MODERN DIGITAL SOLUTIONS

Denysova Lolita[(ADEF)], **Lavrov Vitaliy**[(BCD)]

National University of Ukraine on Physical Education and Sport, Kyiv, Ukraine

Author's contribution:
A – Study design; B – Data collection;
C – Statistical analysis; D – Manuscript preparation;
E – Manuscript editing; F – Final approval of manuscrip

Abstract

Introduction. Esports, characterized by significant exponential growth in recent years, has become a crucial subject of study in the context of the overall dynamics of the video game industry. Simultaneously, there is not only an increased interest in competitive gaming events but also a rise in cybersecurity threats targeting the confidentiality of participants' personal data and the integrity of competitions. These issues pose a substantial threat to the stability and integrity of the esports ecosystem.

The purpose of the study is to investigate and analyze the contemporary digital solutions in the intersection of esports and cybersecurity.

Research methods: the analysis of scientific literary sources and the Internet, generalization, systematization.

Results. The substantial volume of lucrative personal data processed in connection with the participation of virtual players in tournaments with multimillion-dollar prize funds creates new challenges for ensuring confidentiality and preventing unauthorized access. Various types of cyber attacks, such as Distributed Denial of Service (DDoS) attacks, hacking attempts, phishing, and the use of malicious software, using built-in execution proxies to run malicious code, masquerading as legitimate software, and software supply-chain compromise underscore the urgency of developing and implementing effective security measures. Particular attention should be given to proactive cybersecurity management, tailored specifically to the unique requirements of esports, aiming not only to maintain trust but also to ensure the sustainable growth of this crucial industry.

Conclusions. Identified priority directions for the development of cybersecurity systems include aspects of access control with the expansion of authentication procedures, the design of secure systems, the use of cryptographic algorithms like OpenSSL, tracking and analyzing potential threats and malware, migration to cloud platforms that natively offer sophisticated security capabilities, as well as the implementation of cyber insurance. These measures are aimed at establishing a highly efficient and resilient cyber infrastructure, contributing to the enhancement of security levels and the development of the esports ecosystem.

Key words: esports, cybersecurity, data protection, esports ecosystem.

КІБЕРСПОРТ ТА КІБЕРБЕЗПЕКА: СУЧАСНІ ЦИФРОВІ РІШЕННЯ

Денисова Лоліта[(ADEF)], **Лавров Віталій**[(BCD)]

Національний університет фізичного виховання і спорту України, м. Київ, Україна

Внесок автора:

A – концепція та дизайн дослідження; B – збір даних;
C – аналіз і інтерпретація даних; D – написання статті;
E – редагування статті; F – остаточне затвердження статті

Анотація

Актуальність. Кіберспорт, який в останні роки відзначається істотним експоненційним ростом, стає важливим об'єктом дослідження у контексті загальної динаміки розвитку індустрії відеоігор. В той же час, спостерігається не тільки підвищення інтересу до змагальних геймінгових заходів, але й зростання кількості загроз кібербезпеці, орієнтованих на конфіденційність особистих даних учасників та цілісність і чесність змагань. Ці проблеми становлять серйозну загрозу для стабільності та інтегритету кіберспортивної екосистеми.

Мета дослідження полягає у вивченні та аналізі цифрових рішень кібербезпеки в області кіберспорту.

Матеріал і методи: аналіз наукових літературних джерел та мережі Інтернет, узагальнення, систематизація.

Результати. Значний обсяг прибуткових персональних даних, який обробляється у зв'язку з участю віртуальних гравців у турнірах з багатомільйонними призовими фондами, створює нові виклики для захисту конфіденційності та запобігання несанкціонованому доступу. Різноманітні види кібератак, такі як розподілені атаки на обслуговування (DDoS), хакерські атаки, фішинг, використання вбудованих проксі-серверів для запуску шкідливого коду, маскування під легітимне програмне забезпечення акцентують насущність розробки та впровадження ефективних засобів захисту. Особливу увагу слід приділити проактивному управлінню кібербезпекою, адаптованому спеціально для унікальних вимог кіберспорту, з метою не лише підтримання рівня довіри, а й забезпечення стійкого зростання цієї важливої галузі.

Висновки. Визначені пріоритетні напрямки розвитку систем кібербезпеки, включаючи аспекти контролю доступу з розширенням процедури аутентифікації, проєктування безпечних систем з використання криптографічних алгоритмів OpenSSL, відслідковування та аналіз потенційних загроз та шкідливого програмного забезпечення, перехід на хмарні платформи з надійними системами безпеки, а також впровадження кіберстрахування. Ці заходи спрямовані на створення високоефективної та стійкої кіберінфраструктури, сприяючи тим самим підвищенню рівня безпеки та розвитку екосистеми кіберспорту.

Ключові слова: кіберспорт, кібербезпека, захист даних, екосистема кіберспорту.

Introduction

With the rising popularity of esports comes an escalation in cybersecurity threats associated with this sector. Cybercriminals may target players, esports organizations, and enthusiasts using various attack methods, including hacks, fraud, and data breaches. Consequently, the need for modern digital solutions to address cybersecurity challenges becomes more critical [5, 9].

A lot of scientific research are devoted to the current problems of esports, namely: the formation and development of esports in the world and in Ukraine (Y.Imas, O.Yarmoliuk), the system of training and competitions in esports disciplines (O.Shynkaruk), issues of physical activity and injury prevention (O.Andrieieva, M.Dutchak), medico-biological and medical support in esports (L.Shakhlina, S. Futorniy, O.Maslova), analysis of the esports market in times of growing investment attractiveness (Y.Chayka) [2, 3, 9].

The problems of cybersecurity in esports are insufficiently covered in the current literature. There is a need for a more in-depth study of social, economic, ethical aspects of cybersecurity in esports, development and implementation of effective cyber protection strategies.

Aim of the study

The aim of the study is to investigate and analyze the contemporary digital solutions in the intersection of esports and cybersecurity.

The research aims to understand the evolving challenges within this space and provide insights into effective measures to address them.

Material and methods

Methods are the analysis of scientific literary sources and the Internet, generalization, systematization.

Results

Esports, as a form of competitive activity in video games, is gaining substantial popularity, attracting a broad audience and leading to a significant surge in online engagement [3, 9].

In recent times, there has been remarkable expansion in the field of esports due to the increasing acknowledgment of competitive video gaming in the mainstream. Nevertheless, accompanying this surge in popularity, there is a concurrent rise in cybersecurity risks that focus on compromising sensitive data and undermining the integrity of competitions.

As B. Akhmetov states in his work [1], in connection with the growing number of complex targeted cyberattacks directed at the mission critical computer systems, one of the vital problems of society is the information security and its components – cybersecurity. When conducting targeted attacks, cybercriminals frequently are used unique harmful programs and methods of penetrating the objects of cyber protection.

Sheppard Mullin's Privacy and Cybersecurity Team Leader L. Thomas and its Privacy and Cybersecurity Lead Associate J. Kadish discusses the complex landscape of privacy laws in competitive video gaming [10]. They highlight that for stakeholders in the esports industry, data use opportunities must be balanced with a complex web of privacy laws.

New immersive experiences in esports using virtual and augmented reality technologies are increasing the

need for a workable privacy and cybersecurity framework in this area.

As A. Whaley, senior technical director at Promon, points out, from a developer or publisher's perspective, gaming-related cybercrime is detrimental to business. Failure to provide players with a safe and secure experience undermines consumer confidence, undermines in-game economies, and ultimately reduces game and microtransaction sales [15].

According to G. Miller [8], the majority of PC games are delivered through digital platforms, such as Steam, and users ultimately store their credentials in these platforms (including bank information). Thus, digital platforms like Steam, EA Origin, Blizzard's Battle.net, and a handful of other digital game clients are ripe for malicious attacks. Steam alone has over 125 million users. Also at risk are game-specific clients, such as Garena's League of Legends.

F. Mercês and M.R. Fuentes [6] predict that cybercriminals will increasingly target the esports industry over the next years. Through analysis of the esports market and the technology behind it, they believe that it will face the same types of cyberattacks that the gaming community is already facing — but on a larger scale. Also, with esports predicted to join the Olympics in the future, new challenges lie ahead — matches among nations might inspire nation-sponsored hackers to rig games for pride and bragging rights [6].

Esports and cybersecurity are intertwined in today's digital landscape. As eSports continues to grow in popularity and the industry's digital presence expands, cybersecurity has become a top priority for teams, players and tournament organizers. In this context, it is relevant to introduce modern digital solutions to protect the integrity and security of the esports ecosystem [5, 9].

Analysis of sources on the research problem allowed us to identify common cybersecurity threats in the gaming industry [12, 13, 14].

Phishing is one of the biggest cybersecurity threats in esports and online gaming platforms. Phishing campaigns often target clients of gaming platforms to obtain their credentials or payment card information in order to pass it on to other cybercriminals. In some cases, these phishing campaigns are also used to spread malware.

For example, Elastic Security Labs reveals that BLISTER, which is a malware loader associated with financially-motivated intrusions, relied on the rundll32.exe proxy built into every version of Microsoft Windows to launch their backdoor this year.

The BLISTER loader is a useful example because its authors invested a great deal of energy encrypting and obfuscating their malicious code inside a benign application. They fraudulently signed their "franken-payload" to ensure human and machine mitigations didn't interfere.

We often encounter data leaks related to online gaming companies offered and shared on various criminal forums. The players' personal and financial information and login credentials are on sale in most cases. However, besides the players' personal information, the source code for an entire game or some platform databases may be offered for sale and taken by the highest bidder on the dark web.

DDoS attacks

DDoS (Distributed Denial-of-Service) attacks are the most common malicious

campaigns to sabotage an esports event. Hackers can route Internet traffic to servers hosting esports tournaments and matches by slowing them down and overloading them. As a result of a DDoS attack, the connection slows down, and the response time increases, which can easily cause the affected team to lose (see Fig.1).

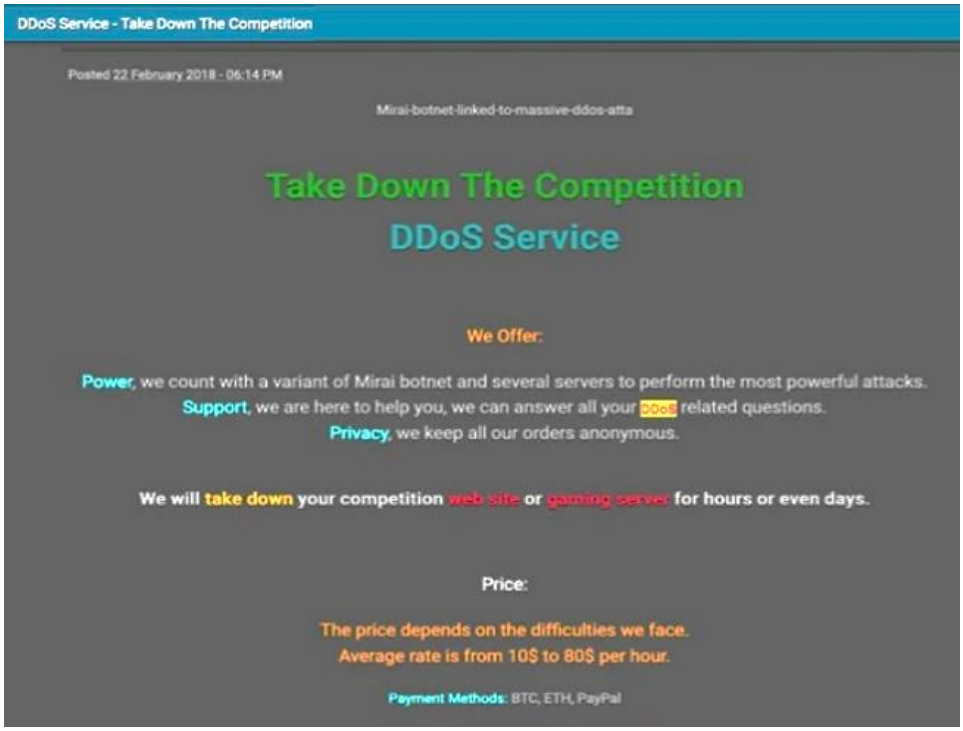


Figure1 – **Illegitimate DDoS offer in the underground market (example)** [4]

A virtual private network (VPN) is one of the most critical security tools: a VPN encrypts your Internet connection and hides your IP address to protect your online activity from hackers.

Many players use it to cover up their real whereabouts and defend themselves against possible DDoS attacks.

Stolen accounts

Hackers often target esports accounts to hack them and exclude owners from their accounts. They also use password cracking software to decrypt account credentials and crack the account.

Theft of intellectual property

One of the main concerns for online gaming companies is intellectual property theft. Gaming companies that have suffered a cyber attack are often involved in the development of games. Creating a single product requires not only a large volume of capital investment but also intellectual capital.

High-value game programs and accumulated intellectual capital (source code of a game) are desirable targets for hackers or players involved in corporate espionage.

Attempts to unfairly manipulate tournament out-comes through hacking in-game environments, exploiting software vulnerabilities, using unauthorized external aids like aimbots etc. fundamentally undermine competitive integrity [7].

Hacking

In online games, hacking is also a widespread problem, and hacking can have two forms. With a keyboard capture feature, Trojans can record keystrokes and the sequence of user actions and then send the recorded password information and data to the current Trojan controller to complete the hacking operation.

Hardware hacks

In professional tournaments, players may bring their own hardware, such as a mouse or keyboard. This also provides an opportunity for fraud: in 2018, for example, a player named "Ra1f" cheated in the Counter-Strike: Global Offensive competition, where he could bypass ESEA anti-fraud technology with his hardware.

The number of methods is almost inexhaustible, insurmountable: more and more ideas come to the surface so that others can be tricked by hackers to obtain their data and thus gain an advantage or money.

In addition to manipulating and hacking virtual data, server maintenance is one of the most common security threats in online gaming.

Server maintenance must generally pass specific parameters to achieve standard access procedures. The admin staff should pay special attention to the verification operation when the server is under maintenance and check that these parameters are valid.

Vulnerable game servers will always be a popular target for hackers. By their nature, servers are almost always online, further increasing their exposure to cyber attacks. Direct attacks on servers are one of the most efficient ways to disrupt esports games and steal information.

The most common attack types and their effects

The most common types of threats can vary depending on whether they are related to professional players, gaming companies, or tournaments. The following figures 2a, 2b summarize the types of attacks and their effects on game companies (TrendMicro).

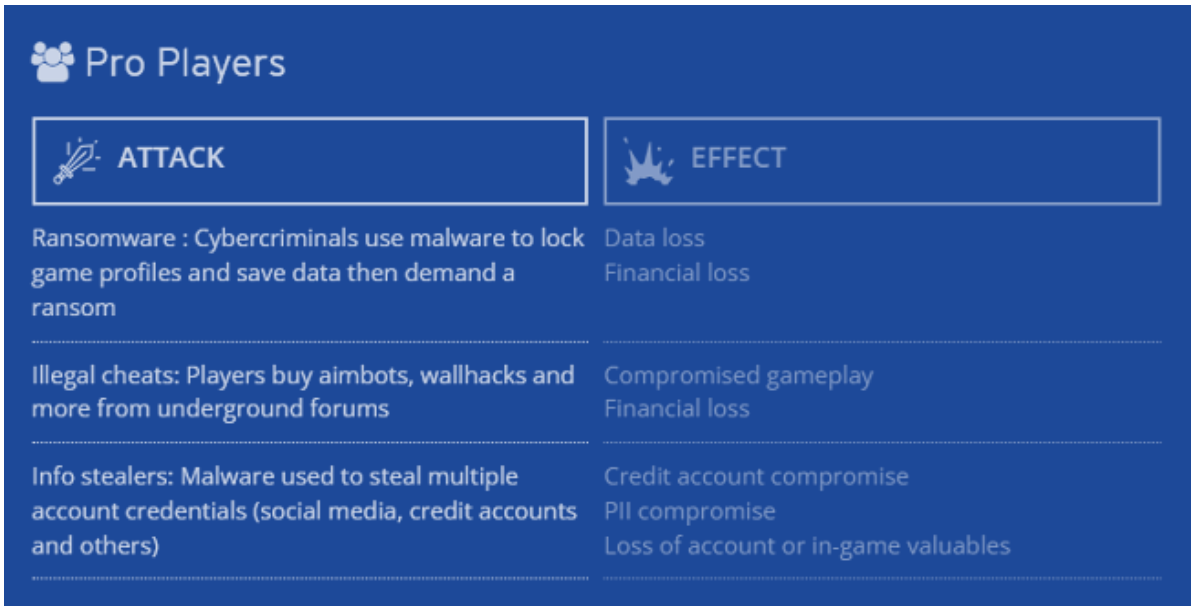
The 2023 Global Threat Report from Elastic Security Labs identified the following factors as a response to security innovations that make the environment hostile to threats [16]:

1) Heavy adversary investments in defense evasion like using built-in execution proxies to run malicious code, masquerading as legitimate software, and software supply-chain compromise.
2) Significant research devoted to bypassing, tampering with, or disabling security instrumentation.
3) Increased reliance on credential theft to enable business email and cloud-resource compromise, places where endpoint visibility is not generally available.

Modern digital cybersecurity solutions for esports include [11, 13, 14]:

- Implementing a proficient data encryption system is crucial for addressing the information security risks associated with the game. Utilizing OpenSSL, with its extensive and powerful features such as cryptographic algorithms, SSL protocol, and certificate package-management capabilities, is essential for establishing and maintaining effective data protection.

a)



b)

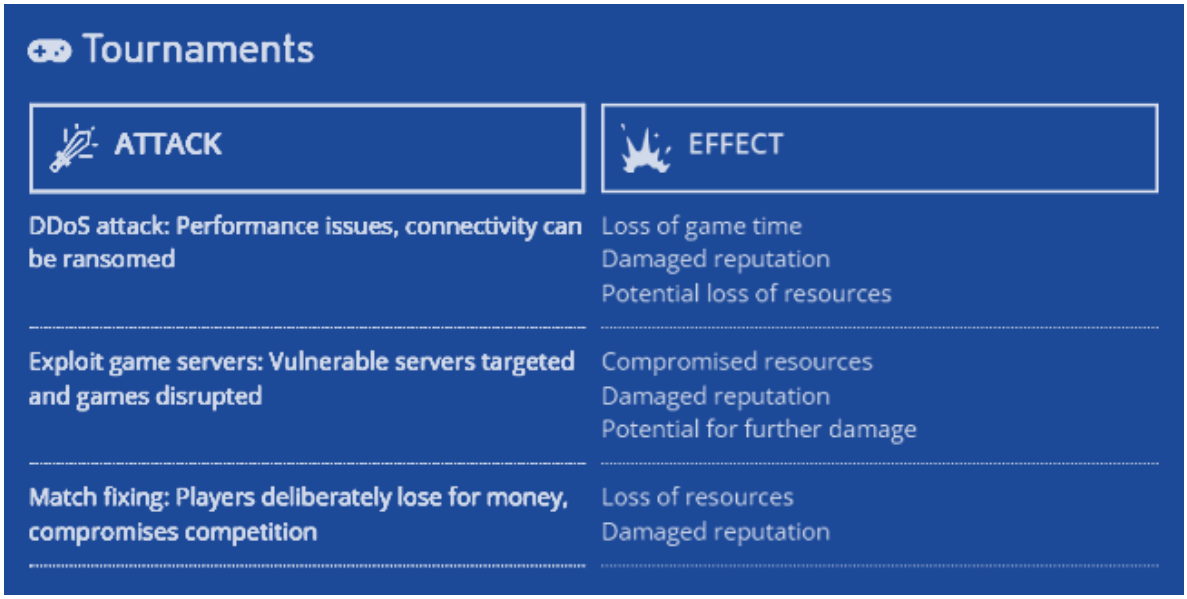


Figure 2 – **The most common attacks and their effects on professional players (a) and tournaments (b)** [14]

- Use of advanced authentication procedures. Employing sophisticated authentication processes is crucial to verify that only authorized players are connected to the server. To ensure the security of network information in the game, it is imperative to incorporate advanced identification technology. During encryption, multiple servers share a common public key, and each system possesses a unique private key for decryption.

- High performing server and wide bandwidth. Ensuring the provision of adequately high-performance servers and broad bandwidth is essential for securely and seamlessly serving players and their requests. Network stability plays a pivotal role in the smooth operation of online games. To mitigate server downtime and potential cybersecurity risks to the game, it may be necessary to deploy additional high-performance servers.

- The Login Gate is primarily used for network communication between the player and the client during login, handling tasks such as encryption, decryption, and verification of communication data between the client and the Login Server.
- Using a VPN is among the most straightforward ways to secure laptop, phone, or console, and it poses a reduced risk when participating in esports events. Despite the abundance of VPN options available, selecting a professional service is recommended, as it not only enhances protection against cyber threats but also ensures the necessary bandwidth, speed, and latency for optimal gaming performance. In addition to shielding users from potential abuse, VPNs can contribute to boosting or stabilizing internet speed and overall performance.
- Building internal capacity through hiring security experts and ongoing training is a core imperative. Migration to cloud platforms that natively offer sophisticated security capabilities provides flexibility. Collaborative mutual defence efforts, such as threat intelligence sharing, collective integrity actions, and incident response agreements, prove force multipliers.

Conclusions

Competitive esports represents an intricate, technology-driven ecosystem with immense volumes of sensitive data in motion and at rest across stakeholders like players, teams, leagues, vendors and broadcast partners.

Its blend of extensive sensitive personal data, competitive insight assets, interconnected network infrastructure and complex fan engagement ecosystems poses immense cybersecurity challenges.

The analysis highlighted the importance of implementing a well-designed data encryption system, utilizing advanced authentication procedures, Private Networks (VPNs) in providing a secure environment for players and deploying high-performing servers with wide bandwidth to secure the network infrastructure of esports.

The insights derived from this research are pertinent to the ongoing development of esports and its cybersecurity framework. As esports continues to gain momentum, the integration of these digital solutions becomes paramount for sustaining a secure and resilient environment.

References:

1. Akhmetov B, Lakhno V, Boiko Y, Mishchenko A. Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. V: *Vostochno-Evropejskij zhurnal peredovyh tekhnologij*. 2017:1(2):4-15. URL: http://nbuv.gov.ua/UJRN/Vejpte_2017_1(2)__2 (accessed: 18.12.2023).
2. Denysova L, Bishevec N, Shinkaruk O. Osnovni ponyattya kibersportu ta tendenciї jogo rozvitku. V: Innovacijni ta informacijni tekhnologiї u fizichnij kul'turi, sporti, fizichnij terapiї ta ergoterapiї. Materiali II Vseukr. elektron. konf. z mizhnar. uchastyu. Kiїv: NUFVSU; 2019:275–6.
3. Chajka Y. Stan ta dinamika rostu rinku kibersportu. V: Ekon. visn. Nac. tekhn. un-tu Ukraïni "KPI". Kiїv: 2018: 15: 443–52.
4. Current and Future Attacks Threatening Esports. URL: https://www.trendmicro.com/en_us/ research/ 19/j/current-and-future-hacks-and-attacks-that-threaten-esports.html (accessed 07.01.2024).
5. Esports and its cyber threats. Luxembourg House of Cybersecurity (2022). URL: http://surl.li/psqas (accessed 07.01.2024).

6. Fernando Mercês. Threats to the Esports Industry in 2019 and Beyond. Trend Micro Research. URL: http://surl.li/qzjio (accessed: 18.12.2023).
7. Freeman, W. (2022, September 20). EA data breach: FIFA and NHL logins stolen and sold online. BBC. URL: https://www.bbc.com/news/technology-62943453 (accessed 07.12.2023).
8. George Miller. The role of cybersecurity in eSports. EuropeanGaming.eu. URL: https://europeangaming.eu/portal/latest-news/2019/02/26/39683/the-role-of-cybersecurity-in-esports/ (accessed: 18.12.2023).
9. Kibersport: monografiya [Andreeva O., Anohin E., Bekar S., Denysova L. ta in. / zag. red. Є. V. Imasa, O. V. Borisovoï, O. A. SHinkaruk]. K.: Olimp. l-ra: 2021: 616 p.
10. Liisa Thomas, Julie Kadish. Playing with privacy? Privacy and cybersecurity considerations in esports. Esports Insider: 2021. URL: https://esportsinsider.com/2021/06/playing-with-privacy-privacy-and-cybersecurity-considerations-in-esports (accessed: 16.11.2023).
11. Mayra Rosario Fuentes, Fernando Merces. Current and Future Attacks Threatening Esports. URL: http://surl.li/psqaw (accessed 27.12.2023).
12. Newzoo (2020). URL: https://newzoo.com/insights/trend-reports/newzoo-global-esports-market-report-2020-light-version (accessed 07.10.2023).
13. Sidikov R. The current landscape of cybersecurity in cybersports. V: Universum: *Ekonomika i yurisprudenciya: elektron. nauchn. zhurn*. 2023:12(110). URL: https://7universum.com/ru/economy/ archive/item/16254 (accessed 07.10.2023).
14. Threats to the Esports Industry in 2019 and Beyond. URL: https://www.trendmicro.com/vinfo/us/ security/news/cybercrime-and-digital-threats/ cheats-hacks-and-cyberattacks-threats-to-the-esports-industry-in-2019-and-beyond (accessed 07.10.2023).
15. Whaley A. Hackers, Fraudsters and Thieves: Understanding Cybersecurity in the Gaming Industry. URL: https://www.infosecurity-magazine.com/opinions/hackers-cybersecurity-gaming/ (accessed 17.12.2023).
16. 2023 Elastic Global Threat Report. URL: http://surl.li/psqaj (accessed 09.12.2023).

The authors claim no conflict of interests.

Author's information:

Denysova Lolita,

Doctor of *Pedagogical Sciences*,
Professor of e-sports and information technologies department,
National University of Ukraine on Physical Education and Sport,
Kyiv, Ukraine
ORCID: 0000-0002-7045-9912
E-mail: kineziology@gmail.com

Lavrov Vitaliy,

Chief Digital Transformation Officer,
Deputy Minister of Ministry of Youth and Sports of Ukraine,
Kyiv, Ukraine
ORCID: 0000-0002-5368-2901
E-mail: Lavrovfz@gmail.com

Received: 03.02.2024 Accepted: 17.02.2024 Published: 21.03.2024

Denysova Lolita, Lavrov Vitaliy. Esports and cybersecurity: modern digital solutions. *Sport Science and Human Health*. 2024;1(11):5-13.
DOI:10.28925/2664-2069.2024.11