Список литературы

1. Батаева Б. С. Развитие корпоративного управления с помощью сервисов электронного голосования // Управленческие науки. 2020. № 2.
2. Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация // Право и политика. 2020. № 9.
3. Габов А. В. Электронное взаимодействие и цифровые технологии в корпоративном управлении акционерным обществом в России // Право. Журнал Высшей школы экономики. 2021. № 2. С. 24–64.
4. Гутников О. В. Тенденции развития корпоративного права в современных условиях // Журнал российского права. 2020. № 8.
5. Долинская В. В. Новеллы гражданского законодательства о собраниях и их решениях // Вестник Университета имени О. Е. Кутафина. 2021. № 11(87).
6. Ельникова Е. В. Использование цифровых технологий при голосовании на общем собрании участников (акционеров) хозяйственного общества // Вестник Университета имени О. Е. Кутафина. 2020. № 7(71).
7. Лаптев В. А. Извещение участников о проведении общего собрания: юридическое значение и последствия // Актуальные проблемы российского права. 2023. № 8(153).
8. Матыцин Д. Е. Правовые конструкции сделок, используемые по особым информационным технологиям для минимизации конфликтов в инвестиционных отношениях // Труды Института государства и права РАН. 2022. № 1.
9. Осипенко О. В. Управление предпринимательскими структурами в России в контексте преодоления коронавирусного карантина // Современная конкуренция. 2020. № 4(80).
10. Бегишев И. Р. Криминологическая классификация роботов: риск-ориентированный подход // Правоприменение. 2021. Т. 5, № 1. С. 185–201. EDN: TBUVGY.
11. Пушкарев С. В. Развитие корпоративного права под влиянием вызовов цифровой эпохи // Инновационные технологии управления и права. 2021. № 1(30). С. 28–32. EDN FZCGQZ.

С. С. Близнякова,
бакалавр,
Санкт-Петербургский государственный университет

ОБЗОР ТРЕНДОВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ, СВЯЗАННОЙ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Статья посвящена анализу современных угроз, которые представляет злонамеренное использование технологий искусственного интеллекта в киберпреступлениях, а также обзору международного сотрудничества по противодействию такого рода преступлениям.

Ключевые слова: киберпреступность, кибербезопасность, злонамеренное использование искусственного интеллекта, уголовное правосудие, Интерпол, ЮНОДК, Будапештская конвенция

OVERVIEW OF TRENDS IN COUNTERING ARTIFICIAL INTELLIGENCE-POWERED CYBERCRIME

Abstract. This article analyses the current threats posed by the malicious use of artificial intelligence technologies in cybercrime, as well as international cooperation to counter such crimes.

Keywords: cybercrime, cybersecurity, misuse of AI, criminal justice, Interpol, UNODC, Budapest Convention

In the last decade, solutions based on artificial intelligence (AI) have deeply integrated in our lives. It is likely that this trend will continue to grow in popularity over the next 10 years: AI solutions are already being integrated not only into routine tasks, but are also widely used in the performance of some particularly important government tasks, such as ensuring national security. Thus, a number of governments uses AI to tackle the challenges of countering (detection and prediction) cybercrime [10]. In addition, machine learning technologies can create AI capable of securing critical infrastructure. Such AI is actively used by the US Department of Energy, which has the most powerful supercomputers in the world to secure critical infrastructure. Moreover, national security and intelligence agencies have recognized the potential of AI technologies to assist in achieving objectives related to national and public security [3]. Today, many governments are successfully working on creation worldwide legislation to regulate particularly sensitive cybersecurity issues.

Since the COVID-19 pandemic, organized criminal groups have significantly enhanced their crime-as-a-service capabilities, allowing them to generate greater financial gains while minimizing the chances of being detected by law enforcement and held accountable for their actions [14]. For example, hackers use AI technologies to scan networks, find vulnerabilities and then attack; resort to social engineering using AI to generate more convincing and personalized phishing emails; and create malware. In general, cybercrime is being democratized as more and more powerful algorithms fall into the hands of inexperienced hackers. It is important to note that the offences continue to involve experienced hackers hired anywhere in the world via Internet.

To counter AI-related cybercrime and obtain cybersecurity as a whole, international applicable instruments are used. Such instruments may be considered as legal frameworks, treaties, agreements, and guidelines established by countries or international organisations that facilitate cooperation, coordination, and effective responses to cybercrime across borders.

The aim of this study is to explore the emerging problem of AI-related cybercrime during 2019-2024, and to analyse global responses to obtain cybersecurity. So, this study revolves around four key objectives:

1. To make a review of AI-powered cybersecurity trends in world;
2. To give possible vectors of strategic partnership between inter-governmental organisations on countering AI-powered cybercrime;
3. To signify international applicable instruments to counter AI-powered cybercrime;
4. To outline the ongoing work of international organisations in terms of international cybersecurity cooperation.

The landscape of digital threats has undergone a profound transformation over the past few decades, driven by technological advancements and the digital interconnectedness of the world. As society increasingly relies on digital technology for communication, commerce, and critical infrastructure, the threat landscape has evolved in complexity and sophistication.

Artificial Intelligence as a Tool

Artificial Intelligence now wields a dual-edged influence reshaping the cybersecurity landscape. This dynamic necessitates continuous innovation in defence strategies to counteract increasingly sophisticated threats. On the attack front, AI is empowering adversaries with more complex methods such as advanced phishing schemes and deepfakes. Noteworthy incidents include a Russian deepfake of the U.S. Ambassador and a deceptive deepfake impersonating a CFO to prompt an HSBC employee to transfer $25 million [18,20]. A report by cybersecurity firm SplashNext reveals a dramatic increase in these tactics: malicious phishing emails rose by 1,265%, and credential phishing surged by 967% since the fourth quarter of 2022 [18]. Cybercriminals are exploiting generative AI tools like ChatGPT to create highly targeted business email compromise (BEC) and other phishing campaigns. And we are already seeing widespread use of other AI tools like voice cloning services to deliver more impactful social engineering attacks. The rapid evolution of these AI-based threats–in speed, volume, and complexity – signals a pressing need for advanced defensive mechanisms in the cybersecurity sector.

Conversely, AI is also bolstering cybersecurity defences. Through automation and sophisticated AI-based security modules, these tools can detect and take the first steps in responding to threats thus helping security teams respond faster and more efficiently, enhancing cybersecurity resilience. There has been an explosion of AI-related security products over the past 12 months, including both tools leveraging AI to help empower security analysts and tools to help protect employees using AI [8]. Long term, AI-powered security services will accelerate threat detection and prediction, alert aggregation, and behavioural analysis, among other capabilities [ibid]. By integrating these advanced technologies, organisations can establish a more robust and proactive defence mechanism against evolving cyber threats, ensuring greater security and resilience in an increasingly digital world.

Ransomware-as-a-Service. Ransomware is a type of malware cybercriminals use to disrupt a victim’s organisation. Ransomware encrypts an organisation’s important files into an unreadable form and demands a ransom payment to decrypt them. Ransom demands are often proportional to the number of systems infected and the value of the encrypted data: the higher the stakes, the higher the payment. In late 2019, attackers evolved their ransomware tactics to include data exfiltration, commonly referred to as a “double extortion” ransomware attack [1]. In these attacks, if victims choose not to pay the ransom to decrypt the data and, instead, attempt to restore the data from a backup, the attackers threaten to leak the stolen data [ibid]. In late 2020, some ransomware attackers added another attack layer with DDoS tactics that bombard the victim’s website or network, creating even more business disruption, thus pressuring the victim to negotiate [ibid]. Ransomware activity alone was up 50% year-on-year during the first half of 2023 with so-called Ransomware-as-a-Service (RaaS) kits, where prices start from as little as $40, a key driver in the frequency of attacks [11]. Most ransomware

attacks now involve the theft of personal or sensitive commercial data for the purpose of extortion, increasing the cost and complexity of incidents, as well as bringing greater potential for reputational damage. According to IBM's X-Force Threat Intelligence Index, ransomware was the second most common type of cyberattack in 2022 [ibid]. Many experts believe the rise of RaaS has played a role in keeping ransomware so prevalent. Additionally, the 2022 report from Zscaler found that 8 of the 11 most active ransomware variants were RaaS variants [1].

The WannaCry and NotPetya cyberattacks in 2017 spread around the world at an unprecedented rate due to their self-replicating features [23]. Given the growth of ransomware attacks and cybercriminals' ongoing efforts to improve their effectiveness, AI-enabled ransomware attacks with self-propagating capabilities may emerge in the future. Deep neural networks could be used to improve target selection based on specified attributes or to disable defences in target systems, making lateralization easier. Additionally, AI could exacerbate ransomware attacks through intelligent targeting and evasion. Intelligent targeting will find new vulnerabilities through various attack methods and apply the most effective ones to access the system.

Cyberwarfare. There have been several high-profile examples of AI-powered cyberattacks in recent years. One example is NotPetya, considered the most destructive malware ever to be deployed, which caused billions of dollars in damage to companies worldwide. NotPetya spread quickly and efficiently using an AI-powered algorithm that allowed it to infect computers without detection. AI-powered attacks have also been used to target critical infrastructure. For example, hackers used an AI-powered malware called BlackEnergy to attack power grids in Ukraine, causing widespread blackouts and disruption to the country's energy supply [17]. In another example, a UK energy firm was scammed out of £200,000 in 2019 when a hacker used AI to impersonate a CEO's voice in a phone call [4].

Thus, we have identified trends such as the use of AI in cybercrime, increased incidents of RaaS, and cyberwarfare during the years of 2019-2024. AI is increasingly being utilized in cybercrime, enhancing the capabilities of cybercriminals in various ways. Ransomware-as-a-Service represents a significant evolution in cybercrime, democratizing access to sophisticated attack tools. The Russian-Ukrainian conflict has the world on high alert and there have been several attacks associated with the Russian-Ukrainian conflict.

International instruments to counter cybercrime. As cybercrime and particularly AI-powered cybercrime has a strong transnational component, measures are needed to be taken at the international level, as well as at the national level, to counter illegal acts in cyberspace.

The Convention on Cybercrime (Budapest Convention) was adopted far in 2001. So, Chapter III of the Convention on Cybercrime provides a legal framework for international co-operation with general and specific measures [6]:

– International co-operation to combat cybercrime must be comprehensive. This principle allows for an uninterrupted exchange of information at the international level.

– The latter provision establishes the general principle that the rules of Chapter III do not override the provisions of international agreements on mutual legal assistance

and extradition, as well as mutual agreements between the parties or the relevant rules of domestic law relating to international cooperation [ibid].

The negotiations, which began in February 2022 under the Algerian presidency, concluded on 9 August 2024 in New York with the approval of the draft Convention [2]. The Russian Federation, which has been actively promoting the cybersecurity agenda since the beginning of 2019, was the initiator of the establishment of the relevant mechanism in accordance with the UN General Assembly resolution 74/247 as well as the inspiration and leader of the negotiations. During the negotiations, eight sessions were held, attended by representatives of law enforcement and political bodies of more than 160 UN member states. The document provides for the establishment of a 24-hour network of national contact centres aimed at assisting, suppressing and investigating illegal activities in cyberspace. The Convention is designed to create a legal basis for international co-operation in combating cybercrime. The document, developed and approved amidst a tense international situation, was submitted to the 79th session of the UN General Assembly for approval [ibid].

The Road of the United Nations. United Nations Office on Drugs and Crime (UNODC) is active in key areas of criminal justice related to the risks and opportunities arising from new technologies. These areas are dynamic and require adaptation to changing conditions and opportunities.

UNODC engages with national authorities, law enforcement agencies, the public and private sectors and civil society actors to effectively harness the potential of new technologies in justice and to analyse in depth their potential risks, including their impact on human rights.

The International Telecommunication Union (ITU) is a United Nations specialized agency responsible for the regulation of information and communication technologies. The ITU's mandate in the area of cybersecurity and cybercrime is based on decisions taken at formal meetings, including Plenipotentiary Conferences and world assemblies. In particular, Plenipotentiary Resolution 130 reinforced the ITU's role in this area by tasking the Secretary-General and Bureau Directors with supporting Member States, particularly developing countries, in developing effective legal measures to protect against cyber threats [15].

International coordination and cooperation through INTERPOL. Recent serious global cyberattacks and cross-border cybercrimes have demonstrated that few have been investigated and the perpetrators brought to justice. Since the 1980s, INTERPOL has served as the leading international police organisation for the development of global cybercrime capacity and training, as well as the coordination of investigations. Regional working groups have been established in Africa, the Americas, Eurasia (Europe and Asia/South Pacific), the Middle East and North Africa. INTERPOL aims to become a global centre for the detection and prevention of cybercrime through its Global Innovation Complex in Singapore, which houses the Digital Cybercrime Centre. The organisation also supports transnational investigations and provides operational assistance to police in 190 countries. INTERPOL has developed a system for the rapid exchange of cybercrime information through the I-24/7 global police network, which enables the collection, storage and analysis of cybercrime data. Coordinated law enforcement action at the international level is key in the fight against cybercrime, and the I-24/7 network provides the ability for police in one country to quickly call on

experts in other countries for assistance in real time. It is important that investigators can quickly seize digital evidence while it is still available and ensure effective co-operation between jurisdictions when cyberattacks affect multiple countries. Effective global investigations are only possible if law enforcement officials have access to information beyond their borders.

The Digital Crime Centre in Singapore has formed regional cybercrime units around the world and has established international partnerships with various public and private institutions, as well as with members of the private sector and academia. INTERPOL is aware that in the future, cyber experts will not only be employed by law enforcement agencies, but also by private companies and academic organisations.

Thus, the most prominent examples of strategic co-operation in the field of cybercrime interdiction and investigation are the partnerships within the relevant UN agencies and INTERPOL. Such institutions are modernising their techniques and tools to combat cybercrime in line with global cybercrime trends, including those related to the use of AI technologies. It is important to note that INTERPOL and UNICRI have agreed to continue to support the United Nations (UN) and INTERPOL member countries «in a coordinated effort, recognising the unique strengths of each organisation and their complementary areas of expertise» [12].

OUTCOMES. Governments across the globe are increasingly acknowledging the significance of AI-related cybersecurity and are implementing measures to regulate and monitor its advancement. The regulation of measures to combat such offences is evolving at both the national and international levels. A strategic partnership in the creation of comprehensive instruments to combat AI-powered cybercrime within the framework of the UN specialised agencies appears to be the most productive and universally applicable approach. Ongoing work includes further elaboration of normative legal acts to counter cybercrime in accordance with the development of new technologies and AI in particular.

References

1. 2022 ThreatLabz State of Ransomware Report // Zscaler, 2022. URL: https://info.zscaler.com/resources-industry-reports-2022-threatlabz-ransomware-report (accessed on 07.07.2024).

2. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. URL: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on 06.07.2024).

3. Artificial intelligence in crime detection: how it’s useful // American Military University. URL: https://www.amu.apus.edu/area-of-study/information-technology/resources/artificial-intelligence-in-crime-detection (accessed on 06.08.2024).

4. A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. URL: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000 (accessed on 16.08.2024).

5. CBC News: The fight against 'deepfake' videos includes former U.S. ambassador to Russia Michael McFaul. URL: https://www.cbc.ca/radio/thecurrent/the-

current-for-july-20-2018-1.4754632/the-fight-against-deepfake-videos-includes-former-u-s-ambassador-to-russia-michael-mcfaul-1.4754674 (accessed on 16.08.2024).

6. Bokovnya A. Yu. et al. Motives and Objectives of Crime Commission Against Information Security // Ad Alta. 2020. Vol. 10, No. 2 S13. Pp. 7–9. EDN: SCSEBN

7. Cyber Dimensions of the Armed Conflict in Ukraine: Quarterly Analysis Report Q3 July to September 2023 // CyberPeace Institute. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf (accessed on 06.08.2024).

8. Cybersecurity trends in 2024. URL: https://www.bvp.com/atlas/cybersecurity-trends-in-2024 (accessed on 06.08.2024).

9. Cybercrime: the global challenge // International Telecommunications Union. URL: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf (accessed on 15.08.2024).

10. European approach to artificial intelligence. URL: https://digitalstrategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence (accessed on 15.08.2024).

11. IBM X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence (accessed on 10.08.2024).

12. INTERPOL and UNICRI release blueprint for responsible use of AI by law enforcement. URL: https://www.interpol.int/News-and-Events/News/2023/INTERPOL-and-UNICRI-release-blueprint-for-responsible-use-of-AI-by-law-enforcement (accessed on 09.08.2024).

13. ITU-T X.1205, Overview of cybersecurity. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (accessed on 09.08.2024).

14. Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C., Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic // Comput Secur. 2021. Jun., № 105. P. 102248. DOI: 10.1016/j.cose.2021.102248

15. RESOLUTION 130 (Rev. Guadalajara, 2010) Strengthening the role of ITU in building confidence and security in the use of information and communication technologies.

16. Significant Cyber Incidents. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed on 19.08.2024).

17. The Dark Side of AI: The Dangers of AI-Powered Cyber Attacks. URL: https://gibraltarsolutions.com/blog/the-dark-side-of-ai (accessed on 09.08.2024).

18 The fight against 'deepfake' videos includes former U.S. ambassador to Russia Michael McFaul. URL: https://www.cbc.ca/radio/thecurrent/the-current-for-july-20-2018-1.4754632/the-fight-against-deepfake-videos-includes-former-u-s-ambassador-to-russia-michael-mcfaul-1.4754674 (accessed on 19.08.2024).

19. The State of PHISHING 2024 Mid-Year Assessment // SplashNext. URL: https://slashnext.com/wp-content/uploads/2024/05/SlashNext-The-State-of-Phishing-24-Midyear-Report.pdf?utm_campaign=The (accessed on 19.06.2024).

20. ‘New deception tactics’. Employee costs company $25 million after scam call with deepfaked CFO. URL: https://www.hrgrapevine.com/us/content/article/2024-02-05-employee-pays-out-25-million-after-scam-call-with-deepfaked-cfo (accessed on 09.08.2024).

21. Smart policies for smart products: A policy maker's guide to enhancing the digital security of products, Directorate for Science, Technology and Innovation Policy Note // OECD, Paris. 2021. URL: https://www.oecd.org/digital/smart-policies-for-smart-products.pdf (accessed on 10.08.2024).

22. Proportion of incident response cases by region to which X-Force responded from 2021 through 2023. URL https://www.ibm.com/reports/threat-intelligence (accessed on 10.08.2024).

23. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 URL https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (accessed on 10.08.2024)

А. А. Богданова,
студент,
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
А. А. Родин,
студент,
Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)

ПРАВОВЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ТРУДОВЫХ ОТНОШЕНИЯХ

Аннотация. По мере того как искусственный интеллект все шире применяется в различных сферах человеческой деятельности, вопросы юридического регулирования его внедрения в трудовые отношения приобретают особую значимость. В данном исследовании освещаются правовые сложности, связанные с использованием искусственного интеллекта в трудовой сфере.

Ключевые слова: искусственный интеллект, цифровая дискриминация, цифровые трудовые отношения, информационное общество, автоматизация, дистанционный формат работы, цифровизация, рекрутинг

LEGAL ASPECTS OF THE USE OF ARTIFICIAL INTELLIGENCE IN LABOR RELATIONS

Abstract. As artificial intelligence is increasingly used in various fields of human activity, the issues of legal regulation of its implementation in labor relations are becoming particularly important. This study highlights the legal complexities associated with the use of artificial intelligence in the workplace.

Keywords: artificial intelligence, digital discrimination, digital labor relations, information society, automation, remote work format, digitalization, recruiting

Введение. Двадцать первый век – это эра информационного общества, когда технологии искусственного интеллекта (далее – ИИ) становятся неотъемлемой частью различных сфер жизни, включая трудовые отношения. В экономическом