УДК 338.23

КИБЕРБЕЗОПАСНОСТЬ И ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКИ

М. Г. Головенчик[1)], Хуан Хаочэнь[2)], Лу Липин[3)]

[1)] *старший преподаватель, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: goloventchikmg@bsu.by*
[2)] *магистрант, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: haochenh93@gmail.com*
[3)] *магистрант, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: lupeninsula@gmail.com*

Авторами рассмотрен рост киберпреступлений в качестве одной из угроз, возникающей в связи с повсеместным внедрением, а также совершенствованием информационно-коммуникационных технологий. Проанализирован опыт обеспечения кибербезопасности Китайской Народной Республики. Рассмотрена взаимосвязь кибербезопасности и экономической безопасности в условиях развития цифровой экономики.

Ключевые слова: цифровизация; цифровая экономика; киберпреступления; кибербезопасность; экономическая безопасность.

CYBERSECURITY AND ECONOMIC SECURITY OF THE PEOPLE'S REPUBLIC OF CHINA

M. G. Goloventchik[1)], Huang Haochen[2)], Lu Liping[3)]

[1)] *Senior Lecturer, Belarusian State University, Minsk, Republic of Belarus, e-mail: goloventchikmg@bsu.by*
[2)] *Master's Student, Belarusian State University, Minsk, Republic of Belarus, e-mail: haochenh93@gmail.com*
[3)] *Master's Student, Belarusian State University, Minsk, Republic of Belarus, e-mail: lupeninsula@gmail.com*

The authors consider the growth of cybercrime as one of the threats arising from the widespread implementation as well as the improvement of information and communication technologies. The experience of ensuring cybersecurity in the People's Republic of China is analyzed. The interconnection of cybersecurity and economic security in the context of the development of digital economy is considered.

Keywords: digitalization; digital economy; cybercrime; cybersecurity; economic security.

As a result of the rapid development of information technology, we are witnessing the emergence of a digital economy, which is seen as a priority for

most countries. In 2021, the development of China's digital economy reached a record breakthrough. In the white paper "Jointly Build a Community with a Shared Future in Cyberspace", published by the China Academy of Information and Communications Technology, is stated that by 2021, the value of the digital economy had reached 45.5 trillion yuan, accounting for 39.8% of GDP and becoming a major growth engine [1].

Based on the available statistics, we may conclude that the digital economy accounts for an increasing share of China's national economy every year and, as such, is increasingly becoming a core part of the Chinese economy. In turn, the development of the digital economy has affected a large number of sectors of society. Many industries are now implementing such technologies as big data, cloud computing, artificial intelligence and blockchain. Thus, a high degree of interconnectedness has become a major characteristic of today's national digital economy.

However, at present, as statistics show and as noted in the doctrine, "unfortunately it cannot be denied that scientific and technological progress, while providing the benefits of civilization, simultaneously creates significant preconditions for the development of a new type of crime – cybercrime, a significant characteristic of which is the use of modern technical means, information and communication technologies to commit unlawful acts" [2, p. 117].

Without network security, there is no adequate level of protection, which means there is a clear risk of a negative impact on economic development. With the rapid development of the digital economy and the growth of remote work caused by the coronavirus pandemic, the possibility of committing cybercrimes, the greatest threat to network security and the digital economy as a whole, has rapidly increased.

By far the most common (but not the only) cybercrime is phishing. According to the Internet Crime Report for 2022, released by the Federal Bureau of Investigation's Internet Crime Complaint Center, phishing, personal data breaches and non-payment/non-delivery are the most common incidents among the complaints received in 2022 [3, p. 21]. At the same time, manifestations of cybercrime in general are multifaceted: cyber extortion, ransomware attacks, information theft, and many others.

It should be noted that the problems of cyber security also affect the economic security of the state. Thus, in addition to the enormous economic damage, the energy sector, the transport system and others are under threat. According to AAG statistics, in 2021 cybercrime cost global economies around $787,671 per hour. Over the course of the year, this amounts to $6,899,997,960 lost worldwide to cybercriminals [4]. These losses include not only direct property losses, but also the sums allocated for remediation and restoration of the original economic system of the enterprise, as well as vari-

ous indirect property losses. At the same time, cybercrimes have a negative impact on public confidence in the state. These negative manifestations have a great impact on the national economy as a whole.

Due to the above-mentioned negative aspects stemming from the online space, cybersecurity is becoming an integral part of the national policies of almost every country. The level of cybersecurity of the state and its bodies directly affects the security of the state as a whole (its bodies, institutions and etc.), and in particular its legal entities and citizens. This requires comprehensive protection from illegal processing of personal data, cyber-fraud, distribution of private content and other threats.

In order to counter cybercrime, it seems necessary, on the one hand, to improve the legal regulation of social relations in the digital environment, and on the other – to improve the technical means to effectively prevent the committing of cybercrimes. Moreover, states, in order to counter various forms of threats to economic relations entities, form special cybersecurity units, departments whose activities are directly related to ensuring digital resilience of both the state and its bodies and organizations, as well as prevention of cybercrime. Among the main responsibilities of these units are to detect cybercrime, eliminate it and enforce the criminal law against cybercriminals in an unstoppable manner.

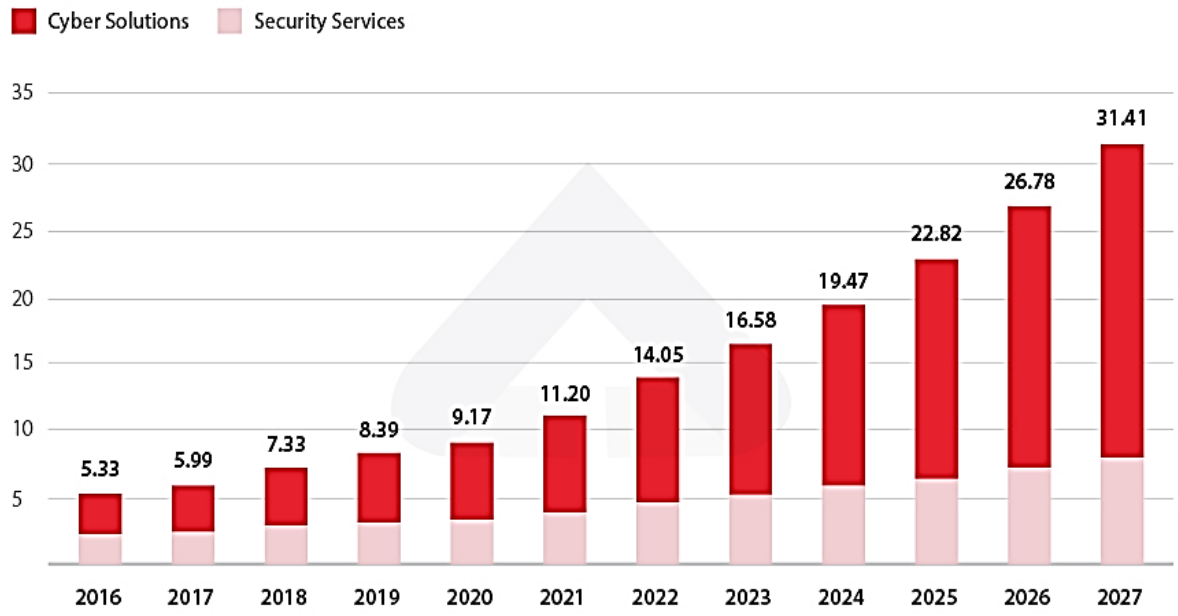
In the People's Republic of China (hereinafter – PCR), issues of ensuring cybersecurity and countering cybercrime are given high priority at the government level. Among the main regulatory authorities are: the Cyberspace Administration of China, the Ministry of Industry and Information, the Ministry of Public Security, the State Administration for Market Regulation and others. It should be mentioned that the newest PRC's national unit is the National Cybersecurity Talent and Innovation Base, which is viewed as a major component of China's response to its cybersecurity problem. The NCC will improve China's cyber capabilities by focusing on two goals: cultivating talent and spurring innovation [5, p. 7].

Besides, the Chinese government has adopted a number of regulatory measures aimed at enhancing network security, including the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, the Network Security Review Measures, the Key Information Infrastructure Security Protection Regulations and others.

In addition, in the Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021–2023) is stated that cybersecurity investments in key industries such as telecommunications will account for 10 % of investments in informatization [6, p. 5]. Moreover, in the country, network security services have become the fastest-growing area of the market

as businesses allocate a higher budget for their security spending to cyber security services.

By 2027, the Chinese cybersecurity market is expected to grow at a compound annual growth rate (CAGR) of about 12.4 % (figure).



China cybersecurity market revenue by segment, 2016–2027 (in billion USD)
Source: [7].

Thus, on the example of the PRC is showed that ensuring cybersecurity is considered as a high priority of the state. Nowadays, cybersecurity issues are of strategic importance for every state in the world as a factor in ensuring security and effective development of the digital economy and other spheres. The importance of the described problems requires the development of a strategy based on the interconnectedness of national and international security, socio-economic development of the country and information security of the state. In connection with the above, it seems necessary to take measures to counter and prevent existing and new threats in cyberspace, both at the national and international level, in order to comprehensively ensure the security of citizens, legal entities and states as a whole.

References

1. Jointly Build a Community with a Shared Future in Cyberspace [Электронный ресурс] // Chinadaily.com.cn. URL: https://www.chinadaily.com.cn/a/202211/07/WS63687246a3105ca1f2274748.html (дата обращения: 25.03.2023).

2. *Головенчик М. Г.* Современная киберпреступность: вопросы понимания и направления противодействия // Современный мир и национальные интересы Республики Беларусь: Материалы международной научной конференции, Минск, 17 декаб-

ря 2021 года / Редколлегия: Е.А. Достанко (гл. ред.) [и др.]. – Минск: Белорусский государственный университет, 2021. – С. 116–120. – EDN ODGPMH.

3. Internet Crime Report 2022 [Электронный ресурс] // Internet Crime Complaint Center URL: https://s3.documentcloud.org/documents/23707016/2022_ic3report.pdf (дата обращения: 25.03.2023).

4. The Latest 2023 Cyber Crime Statistics [Электронный ресурс] // The American Association of Geographers. URL: https://aag-it.com/the-latest-cyber-crime-statistics/ (дата обращения: 28.03.2023).

5. China's National Cybersecurity Center [Электронный ресурс] // Center for Security and Emerging Technology. URL: https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-National-Cybersecurity-Center-1.pdf (дата обращения: 29.03.2023).

6. Three-Year Action Plan for the High-Quality Development of the Cybersecurity Industry (2021–2023) [Электронный ресурс] // Center for Security and Emerging Technology. URL: https://cset.georgetown.edu/wp-content/uploads/t0381_cyber_3_year_plan_draft-EN.pdf (дата обращения: 30.03.2023).

7. China's Cybersecurity Industry: A Market Analysis [Электронный ресурс] // China Briefing. URL: https://www.china-briefing.com/news/chinas-cybersecurity-industry-a-market-analysis/ (дата обращения: 04.04.2023).