ISSN Print 2786-5150
ISSN Online 2786-5169

UDC 339.94(477:410):[351.86:004.056.5(477)] DOI https://doi.org/10.26661/2414-0287-2023-4-60-14

CYBER SECURITY OF UKRAINE IN THE CONTEXT OF INTERNATIONAL COOPERATION WITH GREAT BRITAIN AND GLOBALIZATION CHALLENGES

Venherska N. S., Sulieimanova A.N.
Zaporizhzhia National University
Ukraine, 69600, Zaporozhzhia, Zhukovsky str., 66
nataljavengerskaja@ukr.net, ayben.suleymanova@gmail.com
ORCID: 0000-0001-8171-8206, 0009-0006-9291-3457

Key words:
cyber security, technologies, network, cyber incident, cyber attacks, strategies, international cooperation, financial assistance, experience

In the conditions of globalization and the rapid development of computer technologies, cyber security is becoming an extremely relevant and important aspect that affects the functioning of society, the economy and the security of countries. Every year, the volume of cyberattacks and cybercrime is increasing, which are aimed at a large number of objects – from government institutions to personal devices of citizens, which prompts countries to look for effective methods of protection. Today, Ukraine faces countless hostile attacks and military threats, cyber security is of utmost importance to ensure the functioning of critical infrastructure, protect national security and provide vital services. Creating a resilient and secure digital environment is critical to successfully countering cyber aggression and maintaining national security in the face of military threats. In the article considered the peculiarities of Ukraine's cyber security in the context of global challenges and international cooperation with Great Britain. Attention is drawn to the need for constant updating of technological means and strategies for effective protection of information and infrastructure. The article describes the main results and effectiveness of cyber security strategies of Ukraine from 2016 to 2021. The successful experience of cooperation between Great Britain and Ukraine in the field of cyber security is highlighted, in particular, the UCP program and financial support for ensuring cyber protection. Measures to strengthen cyber defense based on British experience are proposed. The need for cooperation between various sectors, government structures and private companies to effectively counter cyber threats is noted.

КІБЕРБЕЗПЕКА УКРАЇНИ В КОНТЕКСТІ МІЖНАРОДНОЇ СПІВПРАЦІ З ВЕЛИКОЮ БРИТАНІЄЮ ТА ГЛОБАЛІЗАЦІЙНИХ ВИКЛИКІВ

Венгерська Н.С., Сулєйманова А.Н.
Запорізький національний університет
Україна, 69600, м. Запоріжжя, вул. Жуковського, 66

Ключові слова:
кібербезпека, технології, мережа, кіберінцидент, кібератаки, стратегії, міжнародна співпраця, фінансова допомога, досвід

В умовах глобалізації та стрімкого розвитку комп'ютерних технологій кібербезпека стає надзвичайно актуальним та важливим аспектом, що впливає на функціонування суспільства, економіку та безпеку країн. З кожним роком обсяг кібератак і кіберзлочинності зростає, які спрямовані на велику кількість об'єктів – від державних установ до особистих засобів громадян, що спонукає країни шукати ефективні методи захисту. На сьогоднішній день Україна стикається з незліченною кількістю ворожих атак та військових загроз, кібербезпека набуває надзвичайно важливого значення для забезпечення функціонування критичних інфраструктури, захисту національної безпеки та забезпечення життєво важливих послуг. Створення стійкого та безпечного цифрового середовища має вирішальне значення для успішного протидії кібeрагресії та підтримки національної безпеки в умовах воєнних загроз. У статті розкрито особливості кібербезпеки України в контексті глобальних викликів і міжнародної співпраці з Великою Британією. Звертається увага на необхідність постійного оновлення технологічних засобів та стратегій для ефективного захисту інформації та інфраструктури. В статті описуються основні результати та ефективність стратегій кібербезпеки України з 2016 по 2021 рік. Висвітлено успішний досвід співпраці між Великою

Британією та Україною у сфері кібербезпеки, зокрема, програму UCP та фінансову підтримку для забезпечення кіберзахисту. Запропоновано заходи щодо посилення кіберзахисту на основі британського досвіду. Зазначено необхідність співпраці між різними секторами, державними структурами та приватними компаніями для ефективного протистояння кіберзагрозам.

Formulation of the problem

With the expansion of digital technologies and the Internet, the problem of ensuring cyber security is increasing. The increasing diversity of cyber threats endangers information security, economic development and national security of the country. Hackers use various methods such as phishing, password cracking, and other techniques to break into systems and gain unauthorized access to hidden data, or to achieve personal goals. As a result, cyberattacks lead to large-scale economic and other losses, and cybercriminals continue to improve their technology. Companies lose customers, reputation and incur losses due to business process interruptions as a result of cyber-attacks. The same applies to government structures, military systems, and critical infrastructure, all of which lead to system destabilization and pose a potential threat to public safety. In the conditions of martial law, cyberattacks are used in information warfare, which are directed against individuals, organizations, and the state. Dissemination of disinformation, through media resources, influence on public opinion, becomes the cause of disruption of social stability. Therefore, it is necessary to pay attention to the development of scientific and practical tasks and the implementation of effective cyber security technologies and strategies, to conduct relevant research in the field of cyber threats, to identify vulnerabilities and analyze cyber incidents, to apply new methods of protection, using artificial intelligence and data analysis, as well as advanced systems for responding to cyberattacks, strengthen cooperation between government structures, the private sector and international partners in cyber security.

Analysis of recent research and publications

Issues of cyber security are covered in scientific works by both Ukrainian and foreign scientists, in particular I.V. Kotsiuba, J. Williams, K.M. Kraus, N.M. Kraus, O.V. Shtepa [1], Y.S. Manuilov [2], Z. Sverdlyk [3].

In their work, K.M. Kraus, N.M. Kraus and O.V. Shtepa [1] consider the transformational processes of cyber security for business entities, especially focusing on modern digital enterprises under martial law. Define the main tasks of enterprises in the field of cyber security, in particular, identifying potential threats, preventing cyber incidents and minimizing threats to information security.

Scientific work Y.S. Manuilov [2] is devoted to the analysis of the Cyber Security Strategy of Ukraine, which was developed in 2016. The article examines the results of this strategy, the components of the national cyber security system, and evaluates the organizational and legal foundations of cyber security. An analysis of the practical aspects of Ukraine's cyber security strategy and the priority tasks of the security and defense sector is carried out.

Z. Sverdlyk [3] considers the issue of ensuring cyber protection and cyber security in Ukrainian society. Analyzes legislative and regulatory acts that have been adopted in Ukraine recently regarding cyber security. Highlights the need for deepening international cooperation in cyber defense and cyber security issues, as well as the creation of joint interstate platforms for information exchange.

Objectives of the article

The purpose of the article is to reveal the peculiarities of cyber security of Ukraine in the context of global challenges and international cooperation with Great Britain and to develop measures to strengthen cyber protection based on the British experience.

Presenting main material

Let's first consider the essence of cyber security. With the development of digital technologies and the Internet, cyber security has become one of the most important areas of security for the country. Digital transformation, modern technologies, artificial intelligence, cloud computing and the Internet of Things accelerate technological progress, but at the same time create new threats, such as cyber attacks. Cyber attacks can have devastating consequences for the economy and other spheres of activity, threaten national and public security. Ensuring security in cyberspace is a complex process that requires constant updating of technological means, conducting scientific research, developing new methods and strategies, and exchanging information about cyber threats at the international level.

Cyber security is the application of technologies and methods aimed at protecting systems, networks, programs, organizations or countries from crimes and digital attacks [5].

The entry of business into the Internet provided not only opportunities, but also threats. Today, theft of electronic information has become one of the most common frauds, surpassing physical theft. The cyber security of the financial sector and business is a particularly important component, as a huge volume of financial transactions and information can become the object of attacks. Attacks on the financial sector and businesses can have serious consequences for economies, markets and populations. Therefore, it is necessary to introduce modern technologies for processing and storing information, as well as regular training of personnel on cyber security. Cyber threats are constantly evolving and this requires updating security measures. Conducting regular audits and vulnerability testing helps identify weak points and improve security measures. The financial sector and business must also adhere to cybersecurity regulatory requirements and standards to ensure compliance and reduce the risk of a security breach.

The largest cyber security market in Europe is concentrated in Great Britain. It is home to the world's leading cyber companies that enjoy exceptional opportunities to attract talent and investment. The UK provides access to cyber security excellence that helps businesses remain competitive in the global marketplace. The development of the cyber sector in the UK has become a priority task for the country's national security and prosperity. The creation of a national cyber security strategy by the state ensures that the United Kingdom is independent, capable and confident in a world of digital change. The strategy helps the country quickly adapt, introduce new innovations and attract foreign investment to protect and support its interests in cyberspace.

Annually, the UK government conducts a cyber security breach survey as part of the national cyber strategy, which is used by businesses and government to tackle cyber risks and create a safer UK cyberspace. Includes key information from UK businesses, charities and educational institutions on their cyber security policies, processes and overall cyber resilience and cybercrime assessments.

Based on the obtained data presented in the report [9], the share of companies that have experienced cyberattacks remains relatively stable, ranging from 30% to 46%. During the COVID-19 pandemic in 2020, cyber attacks on companies increased again. This may be due to the fact that a large number of companies have actively moved their activities online, which has made them more vulnerable to external threats. In 2023, the share of companies that detected cyberattacks dropped to 30%. The results of the study show that the decrease in cyber attacks is related to the fact that companies implement measures to improve the cyber security system (Fig. 1).

In connection with the beginning of the full-scale invasion, the number and complexity of cyber attacks in Ukraine increased. During 2022, Ukraine faced 7.000 cyber attacks on information infrastructure. Last year, 2.8 times more cyber incidents were registered in Ukraine than in 2021 [11]. In turn, it increases the need to develop innovative methods and strategies to ensure effective protection against cyber threats. This requires constant improvement of cyber security and the introduction of advanced technologies that will guarantee reliable protection of information and infrastructure in the face of growing cyber risks.

As evidenced by the British experience, a component of successful cyber security is cooperation between different sectors, government structures and private companies, joint exchange of information and experience between countries.The UK government actively engages with companies and non-governmental organizations on cyber security issues. The UK's National Cyber Security Center (NCSC) is a key aspect of the UK's national cyber defense strategy, developing collaborative projects with the private sector, academia and other non-governmental organisations. The main goal is to provide support in the field of cyber security, exchange information about threats and jointly solve technical issues.

An example of such cooperation is the partnership with the company Rolls-Royce, which is a well-known manufacturer of aircraft, marine and industrial engines, and also plays an important role in the field of aerospace technology. The main mission of cyber security is to create safe conditions and provide protection against cyber threats. NCSC works with Rolls-Royce to share information on emerging cyber threats, analyze potential cyber attacks and determine the best measures to ensure cyber security in their system. This collaboration allows Rolls-Royce to combat cyber threats and effectively protect its technology, which is essential to ensure the national security of Great Britain [6].

In Ukraine, the first cyber security strategy was approved in 2016 for five years and became the foundation for the development of the country's national cyber security system. However, it had many shortcomings, such as the priorities of state policy in cyberspace were not clearly defined, it focused on the activities of security and defense agencies, and cooperation between the public and private sectors was not included. According to the results of the analysis, the effectiveness of the implementation of this strategy was only 40%. Over the following years, positive changes were observed. In 2017, the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" approved the powers of state bodies, enterprises and individuals

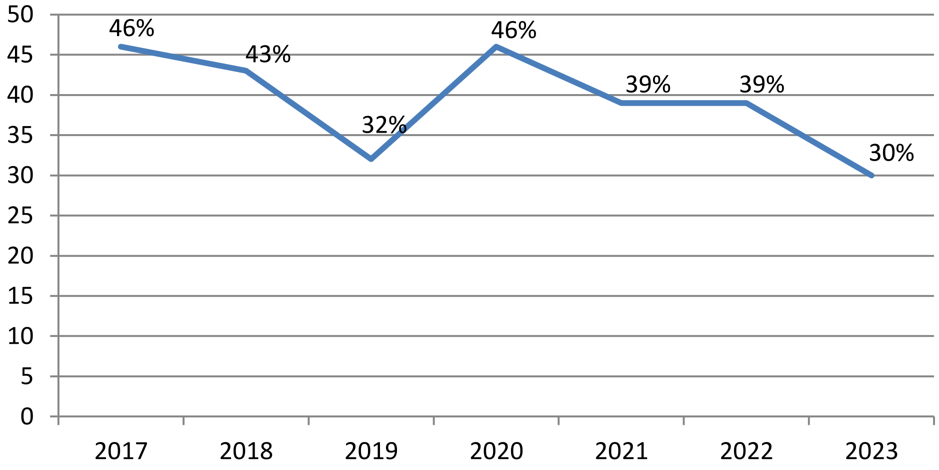

Fig. 1 – Proportion of UK businesses identifying cyber attacks each year

Source: compiled by the author based [9; 10] in the sector. In 2020, cooperation was established at the international level, in state structures, and specialized cyber security units were created. The cyber security strategy of 2021 was approved until 2025, the main goal was to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society, state, and global integration. When adopting the new Cyber Security Strategy of Ukraine, previous experience and problems were taken into account, based on this, a perspective plan for the development of the cyber environment at the national and international level was developed [4].

According to the results of a study conducted by the Cohesity company [12], most enterprises lack the necessary strategies aimed at data protection, which are necessary to counter modern cyber threats and support uninterrupted business operations. From the survey conducted, 93% of business owners confirmed that the number of threats to attack applications in 2023 has increased significantly compared to last year. The problem is that the provision of cyber protection is complicated by the rapid development of cyber threats, the lack of technology and constant data recovery, and the lack of cyber insurance. As a result of the company facing a system-wide cyberattack, the survey participants are confident that the company will not be able to restore data and business processes.

Today, Ukrainian cyber security represents a set of measures and initiatives aimed at protecting cyberspace, information resources, technologies and data in Ukraine, namely transferring data to the cloud, partnering with foreign companies and using the Internet via satellite using Starlink terminals. Ukrainian cyber security includes various organizations and structures, which in turn perform analysis, monitoring, development and implementation of cyber protection measures.

For example, a system for detecting vulnerabilities and responding to cyber incidents and cyber attacks is a set of software tools that provide constant monitoring, analysis and transmission of telemetric information about cyber incidents and cyber attacks that occur or have occurred at informationally protected objects and may negatively affect their functioning [12].

According to the report of the System of Vulnerability Detection and Response to Cyber Incidents and Cyber Attacks [9], during 2022, 2.8 times more cyber incidents were registered in Ukraine than in 2021 (Fig. 2).

The UCP Ukrainian Cyber Security Project, funded by Great Britain, uses advanced international knowledge from both the private and public sectors to protect Ukraine's vital national infrastructure and provide critical public services. This program is aimed at increasing the level of cyber security by using advanced approaches and global experience in this field.

In 2022, the British government allocated 6.35 million pounds to support Ukraine's cyber defense. The program was aimed at protecting critical infrastructures, financial institutions, companies, and government structures from malicious cyber attacks. This partnership provides for limiting the access of Russian hackers to critical networks and provides enhanced forensic analysis capabilities to ensure national security and effective investigation [7].

In June 2023, the UK decided to strengthen cyber defense with a financial aid package of up to £25 million, of which £16 million in UK funding and £9 million from international allies [8].

Great Britain continues to support Ukraine in strengthening its cyber security, and this partnership is positive for our country in the field of cyber security. The introduction of advanced approaches and the use of global experience will contribute to ensuring security and collective long-term stability in this area for the citizens of Ukraine.

Also, one of the examples of Great Britain's support is the cooperation between Durham University and Zaporizhzhia National University. In 2022, the universities signed a partnership agreement aimed at promoting

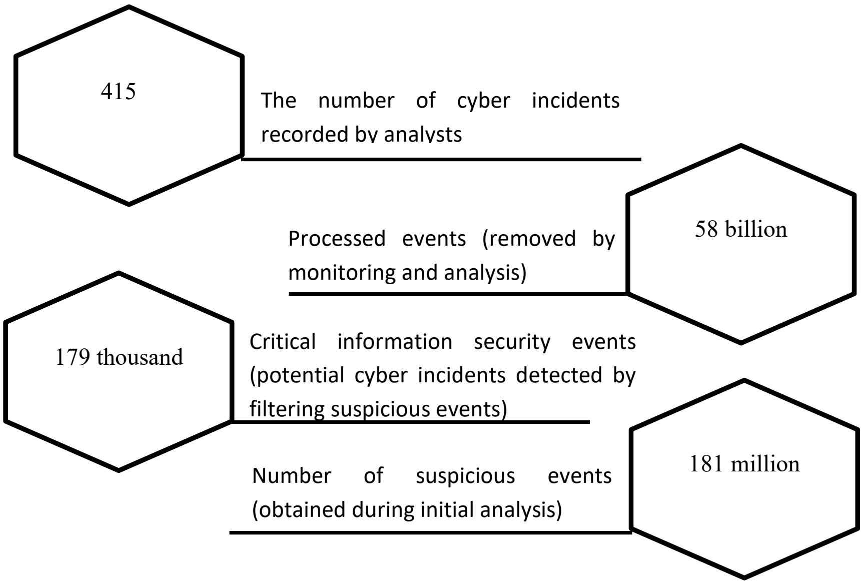
415
The number of cyber incidents recorded by analysts
58 billion
Processed events (removed by monitoring and analysis)
179 thousand
Critical information security events (potential cyber incidents detected by filtering suspicious events)
181 million
Number of suspicious events (obtained during initial analysis)

Fig. 2 – Statistics of cyber incidents and cyber attacks during 2022

Source: compiled by the author based [12] academic mobility, joint research and cultural exchange between the universities. The agreement is carried out within the framework of the "Education and technologies for sustainable development" project. This project is aimed at the development of new educational and technological solutions for solving the problems of sustainable development, restoration and strengthening of Ukraine, as well as for projects in the field of energy, finance, cyber security and other industries. This cooperation is important because it helps Ukrainian students and teachers to conduct joint scientific research and expand educational opportunities, helping to raise the quality of the academic process.

Conclusions

Therefore, in the modern world of technology, cyber security is an integral component for the stable and successful functioning of companies, government and other institutions. With the increase in the scale of cyberspace and the use of the latest technologies, new opportunities appear, but at the same time, risks that can pose a threat to both the country and citizens.

For Ukraine, it is important to create and constantly improve the overall national cyber security strategy, which will capture all spheres of activity and infrastructure. This strategy should include the creation of national cyber security centers, in which efforts will be directed to the detection, analysis and response to cyber threats. To ensure the effectiveness of measures, it is especially necessary to develop a personnel policy and increase the number of qualified cyber security specialists.

Great Britain's experience in this area demonstrates that for the successful implementation of a cyber security strategy, active cooperation with public administration structures and with private companies should be carried out to exchange information about cyber threats and implement advanced technologies. The UK is channeling its resources into educating its citizens, organizations and government officials about cyber security and good behavior in cyberspace, which in turn helps prevent social engineering and phishing.

Considering, based on the experience of the United Kingdom, Ukraine should focus its efforts on creating innovative solutions in the field of cyber security, such as the development and implementation of artificial intelligence, machine learning and automated systems for effective detection and countermeasures against cyber threats.

In summary, cyber security strategies must be flexible and adaptive to ensure an adequate level of protection against persistent threats. Cooperation and innovation are key factors for an effective response to cyber threats, guaranteeing the stability and security of the country's information resources.

References

1. Kraus K.M., Kraus N.M., Shtepa O.V. (2022). Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu – [Digital transformation of cyber security at the micro level in martial law]. *Innovatsii ta stalyi rozvytok.* № 3. P. 26–37. [in Ukrainian]
2. Manuilov Y.S. (2021). Ohliad novel vitchyznianoho zakonodavstva u sferi zabezpechennia kiberbezpeky (na prykladi stratehii kiberbezpeky ukrainy na 2021–2025 roky) – [Review of novelties of domestic legislation in the field of ensuring cyber security (using the example of Ukraine's cyber security strategy for 2021–2025)]. *Informatsiia i pravo.* № 4(39). P. 98–105. [in Ukrainian]
3. Sverdlyk Z. (2022). Kiberbezpeka ta kiberzakhyst: pytannia poriadku dennoho v ukrainskomu suspilstvi – [Cyber security and cyber protection: issues of the agenda in Ukrainian society]. *Ukrainskyi zhurnal z bibliotekoznavstva ta informatsiinykh nauk.* № 10. P. 175–188. [in Ukrainian]
4. Analytical Center ADASTRA. New cyber security strategy: how will Ukraine defend itself in cyberspace? URL: https://adastra.org.ua/blog/nova-strategiya-kiberbezpeki-yak-ukrayina-zahishatimetsya-v-kiberprostori [in Ukrainian]
5. Cambridge Dictionary. The term cyber security. URL: https://dictionary.cambridge.org/dictionary/english/cybersecurity
6. Report on cyber incidents. *Official site of Rolls-Royce*. URL: https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/contact-us/NTS_561_Cyber_ Incident _Reporting.pdf
7. UK boosts Ukraine's cyber defences with £6 million support package. *The official government website of the United Kingdom.* URL: https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package
8. UK to give Ukraine major boost to mount counteroffensive. *The official government website of the United Kingdom.* URL: https://www.gov.uk/government/news/uk-to-give-ukraine-major-boost-to-mount-counteroffensive
9. Cyber security breaches survey 2022. *The official government website of the United Kingdom.* URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
10. Cyber security breaches survey 2023. *The official government website of the United Kingdom.* URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
11. Statistical report on the results of the System for detecting vulnerabilities and responding to cyber incidents and cyber attacks during 2022. *State Cybersecurity Center of the State Special Communications Service.* URL: https://scpc.gov.ua/ua/articles/233
12. Report: 67 Percent of Businesses Lack Confidence of Full Recovery After Cyber Attack. *Group of infrastructure solutions.* URL: https://securitytoday.com/articles/2023/07/31/report-67-percent-of-businesses-lack-confidence-of-full-recovery-after-cyber-attack.aspx?admgarea=cybersecurity