Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

Cyber security in international relations: Risks and prospects

Oleksandra Zinchenko

V.N. Karazin Kharkiv National University

alekca.98@ukr.net

Abstract. The purpose of this article is to determine the essence, theoretical foundations, and legislative aspects of regulating cyber security in international areas, as well as researching risks and prospects for improving cyber security at the international level. The problems of ensuring cyber security at the international level, as well as the key cyber threats that have the greatest damage in the cyber security of the countries of the world, have been studied. The main directions of international cooperation on ensuring cyber security at the international level have been determined. The peculiarities of cyber security of the EU countries are characterized, as well as the legislative acts that regulate this activity and are distributed to all members of the union. The main characteristics of cyber security of the NATO countries and the BRICS association, as well as the peculiarities of cyber security regulation, taking into account the difference in the legal framework of the participating countries, are provided. The characteristics of the cyber security of China, Japan and Great Britain are highlighted, as well as the basics of cyber security of Ukraine are defined: problems and prospects for its further development, probable directions of borrowing world experience in cyber protection of national interests.

Keywords. cyber security, cyber terrorism, cyber space, information technologies, international relations

Introduction

In the modern conditions of mobile development of the global information society, the widespread use of information and communication technologies in all spheres of life, the issue of cyber security takes on special importance. Cyber security cannot be guaranteed without close cooperation with influential security structures at the regional, trans-regional and global levels. Taking care of its own security, each state or group of states should support the development of effective stability mechanisms, considering it as an important element of its national security.

Cyber security is especially relevant in the context of countries participating in the global cyber civilization - the level of development of the information society of humanity and the effectiveness of its components are determined by the achievements of scientific and technical progress, the level of development of computer information technologies as a means of global telecommunications.

Cyber security is achieved by ensuring a balance between the rights and freedoms regarding information concerning various legal subjects and the protection of national information sovereignty. After all, the issue of cyber security and national security as a whole

is, first of all, a question of balance between human rights and interests and the capabilities and interests of state power, a balance that can be established only with the help of legal norms.

A very important aspect in determining the principles of formation and functioning of cyber security systems is the accounting of international legal norms. The main goal of ensuring cyber security should be defined on the basis of a broad understanding of this concept as an important element of national security, a system-forming factor in all spheres of human activity, society, state, politics, economy, socio-cultural, scientific and technical, defense, environmental and informational components of national security.

Cyberspace has become an integral part of the life of a modern country. It contributes to the solution of social problems, has huge potential in terms of economic growth and innovation, and the world community sees it as a stimulus for development and provides opportunities for communication and public relations.

At the same time, cyber attacks on information infrastructure are becoming a real threat and are one of the priorities of national security and risk management.

At the global level, cyber terrorism, cyber espionage and cyber attack activities have become serious threats to international security, military stability and the development of the world economy. Conducting research in this field will help to identify new opportunities and scenarios of development of events in the digital space and will contribute to the formation of strategies for international cooperation in the field of cyber security.

At the regional level, each country faces unique cybersecurity challenges that depend on its geopolitical position, technological development, and defense infrastructure. The study of cyber threats and the development of cyber weapons are becoming very important for the development of national security strategies and the protection of important information.

The effectiveness of intellectual property protection in the digital space of the Internet is determined by its ability to resist similar violations and the threat of their occurrence in the future. The threat of infringement of intellectual property rights in cyberspace (cyber threats) is associated with certain risks and may affect the existence of objects of exclusive intellectual property rights. In particular, as a result of a cyber attack, a database containing specific information that is important both for the development of individual entities and for the development of the entire state may be lost, or information containing commercial secrets may be disclosed. In view of this, an effective system of protection of intellectual property rights is part of cyber security and national security, since it is scientific creativity that is the basis of innovations that allow the state to win competition and lay the foundation for economic and social breakthroughs[1].

Problems of ensuring cyber security at the international level

The problem of ensuring cyber security is becoming the subject of an increasingly wide discussion not only at the national, but also at the international level. This is due to several factors, some of which are listed below.

Factors determining the need for international cooperation in the field of cyber security:

1. Different approaches to understanding cyber security.

Effective cyber security requires a common understanding of its importance in all countries. Cyber security involves protection against unauthorized access, manipulation and

[1] Modern trends in legal regulation of cyber security and intellectual property [Electronic resource]. URL: https://coordynata.com.ua/sucasni-tendencii-pravovogo-reguluvanna-kiberbezpeki-ta-intelektualna-vlasnist

destruction of critical resources and assets, such as data on the activities of banking institutions and government authorities. The cost of such resources and assets varies from country to country. It depends, in particular, on the level of development and type of economic activity, as well as on which countries consider it as a vital resource, and what efforts they are willing to make to ensure their own cyber security. The cyber security needs, priorities and strategies of least developed countries are clearly different from those of developed countries. The variety of positions of major geopolitical players creates conceptual uncertainty regarding the forms and methods of detecting cyberattacks in accordance with international law, which makes it impossible to develop appropriate response measures to such attacks. Therefore, the development of a common vision and action plan for solving the cyber security problem is very important for most, if not all, countries of the world and is possible only with close international cooperation based on new principles corresponding to emerging challenges.

2. Global (cross-border) nature of cyber threats.

The problems associated with cyber threats are of a global nature. But unlike traditional international illegal activity, which in principle can be successfully combated by closing borders, borders are transparent to cyber threats. Time and geographic factors, as well as the location of potential victims, are no longer obstacles to determining the place and time of a cyber attack. Thus, individual countries are practically unable to resist modern threats. All attempts to solve these problems at the national and regional levels proved to be ineffective. Without a doubt, measures to combat cyberattacks at the national and regional levels are necessary, but they are not sufficient to adequately address the latest global challenges. Legal, technical and institutional problems arising in connection with cyber-attacks and cybercrimes, as a rule, lead to serious destructive consequences that affect the interests of many countries and negatively affect all levels of state governance. All attempts to solve these problems at the national and regional levels are ineffective a priori, because cyberspace has no borders and is limited only by human imagination. In addition, there is no need to talk about the correspondence of the boundaries of cyberspace to existing geographical boundaries, so cyber threats can arise anytime and anywhere and cause significant damage in a very short period of time before they are eliminated.

3. Technical features of message routing.

In most cases, several countries are involved in the data transfer process. The protocol used for this is based on the principle of optimal routing when the direct line is temporarily blocked. Data can leave a country even if the internal transfer process within the country of origin is restricted. At the same time, communication is carried out through a router located outside this region and is redirected to the country of final destination. In addition, many modern electronic services are based on foreign services. For example, a hosting provider may offer to rent web space in one country and equipment in another.

4. Short deadlines for investigating cyber incidents and responding to them.

Investigating incidents that occur in cyberspace, as a rule, requires tight deadlines. Important crime tracking data is usually deleted very quickly. The short period of investigation creates problems, as the organization of the traditional mutual legal assistance regime takes a very long time. Formal requirements and the time required to cooperate with foreign law enforcement agencies often make investigations difficult, and in some places even make them inconvenient[2].

[2] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

5. Differences in approaches to ensuring cyber security.

Building cooperation in the field of cyber security based on the traditional principle of mutual legal assistance is very difficult. For example, the principle of mutual recognition of conduct as a crime creates serious difficulties, if in one of the countries participating in the investigation of cyber incidents, this crime is not classified as a crime, then criminals can deliberately use such countries in attacks to complicate the investigation. Preventing the creation of "safe harbors" is one of the main tasks in the field of cyber security. As long as such "harbors" exist, attackers will use them for cyber attacks. It is worth noting that in practice, first of all, developing countries, which have not yet adopted laws on cyber security, are very vulnerable, since criminals, as a rule, choose such countries as their base.

6. Lack of proper organizational structure.

There is also a lack of institutional structures to deal with the consequences of incidents (such as viruses and networks leading to fraud, destruction of information and distribution of prohibited content), and some countries and regions have established their own institutions to monitor, prevent and respond to incidents in cyberspace, and organizational structures to coordinate actions to respond to cyberattacks. However, the current situation in the field of cyber security requires much greater efforts. If a cyberattack occurs in one country, its devastating effects can overtake victims within minutes in the country where the connection is established. Free flow of information and cooperation between national organizational structures are necessary for effective consideration of such incidents and response to them. Another area in which organizational structure and policies need to be developed is in the area of general identity certificates (digital certificates). For a long time, user authentication was considered the most effective strategy for combating cyber threats (theft of personal data, phishing and other types of online fraud). Strict authentication is an important element of strengthening trust and security in the information society. Some countries have established the organizational structure and infrastructure necessary to provide citizens with a single identity card, while others have not yet established such a structure or are just starting to operate [3].

It is worth noting that the activities of the governments of the countries of the world are aimed at ensuring the state of international relations at the level of normal functioning of the world community, stable development and cooperation of peoples, states and interstate associations, protection of their respective vital interests from new threats.

Norms of such activities are formed on the basis of national and regional security. The components of international security are economic, political, ecological, military, informational, cybernetic and other types of security.

International security involves the following:

- all human rights to existence and sustainable development must be protected in the same manner, regardless of the country and its level of development, nationality, religion;
- recognition of the sovereignty and territorial integrity of the state;
- independence and originality of the development of the country and people;
- environmental protection and rational use of natural resources;
- freedom of movement of people, capital and information;
- full rights and equality of citizens, etc.

[3] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

Strengthening of all forms of international cooperation, observance by all states of generally accepted principles based on the UN Charter, etc., as well as norms of international law are still a guarantee of the strength of international security.

Therefore, at the international level, cyber security issues are considered in the following framework:

- The UN adopted a number of decisions, resolutions and recommendations related to cyber security issues;
- the group of eight (G8), which established a subcommittee on combating crimes related to the use of high-tech resources, considers, among other things, the issue of combating cybercrime;
- the Council of Europe, which in 1996 established a commission to combat cybercrime;
- the International Telecommunication Union implements its own global cyber security program.

At the international level, cyber security is a cross-border challenge that cannot be provided by one state or a group of states, it is the work of all civilized countries. Only joint efforts to ensure cyber security will have a significant effect and contribute to increasing the level of international security in cyberspace, both for an individual state and for the entire world community. To achieve such goals, it is necessary to find new ways of building similar international organizations, mechanisms, measures and systems of guarantees. This allows you to minimize the likelihood of cyber threats and neutralize them.

Cyber security at the international level is formed on the basis of national cyber security strategies of individual states, regional (sub-regional) security of groups of states and regions of the world and is integrated into the level of global international cyber security when it comes to cyber protection and realization of universal benefits from planetary threats. Its scope and consequences may affect the security of humanity beyond national borders.

Cyber security at the regional level is a feature of ensuring cyber security at any regional level of the country, on the scale of a group of countries belonging to a certain geographical area, for several adjacent areas, regions of a specific state, restrictions for certain areas in which natural, geographical, social - economic, cultural, historical and other living conditions are different; in a separate part of the social territorial community of people according to the specifics of interests that have developed in a certain habitat; content and forms of manifestation of contradictions between this community and the center, other regions and the world community.

At the regional level, cyber security is implemented on the basis of several principles: territorial organization of cyber protection of the population, places of residence and objects with important information infrastructure; a comprehensive approach to creating a cyber security system within the region; indivisibility of security and sustainable development; continuity of efforts, which involve the organization of constant monitoring and control of the state of society, the natural environment, the protection of potentially dangerous objects, such as targeted cybernetic intervention[4].

Cyber security in some regions cannot be adequately ensured outside of the framework of higher level cyber security systems. However, it should be noted that it is at the regional level

[4] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

that the main foundations of cyber security of interstate companies, states and individuals, as well as their sustainable and stable development, are laid.

Regional security levels:

- another administrative and territorial unit of the country;
- a group of countries belonging to a certain geographical area.

At any level, security is based on national and international security and includes political, economic, environmental, informational, cyber and other types of security.

Areas of regional security include:

- resolving disputes, preventing disagreements between members of the region;
- organization of collective measures to deter acts of aggression and eliminate security threats: preventive diplomacy, support, establishment and strengthening of relations in the post-conflict period.

Regional security, as a rule, is formed with the help of agreements, from which the system of regional security is formed.

At the regional level, cyber security issues are resolved in the following frameworks:

- all member states of the European Union without exception are involved in this process;
- NATO believes that such cooperation primarily concerns the military component of cyber security;
- The Organization for Economic Cooperation and Development has been conducting research in the field of cyber security since 1983 and, on the basis of this, developed a set of measures to increase the level of such security;
- Asia-Pacific Economic Cooperation (APEC) adopted the APEC Cyber Security Strategy in 2002 and committed to help each other in solving cyber security issues in all ways;
- National community, within the framework of which a model law on computers and computer crimes has been developed, which makes it possible to evade bilateral negotiations within the framework of the association on cyber security issues;
- the member states of the League of Arab States and the Cooperation Council of the Arab States of the Persian Gulf declared the need to find a joint approach to solving problems related to cyber security;
- The Association of Southeast Asian Nations has created a cyber security system that covers ten countries of the community and seeks to prevent cyber attacks and other cyber crimes;
- Organization of American States, within which member states resolve general issues of cyber security in the form of an annual meeting of ministers of justice and lawyers and actively cooperate with the G8[5].

Cyber security is guaranteed to protect the state of society, relations, important interests of individuals, society and the state from external and internal threats. The main goals of national security are:

- personality with its rights and freedoms;
- social and national groups, their internal integrity, autonomy, material and spiritual values;
- the state, its constitutional system, sovereignty and territorial integrity.

[5] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

Types of national security differ depending on the area of potential security threats. Its main types are economic, political, ecological, informational, military, etc. Cybersecurity, in particular, stands out and directly affects each species.

At the international level, many countries of the world have recently significantly intensified their activities in the field of cooperation in the field of cyber security. Many bilateral agreements were signed between different countries. However, given that the main participant in bilateral cooperation in this direction is the United States and that all spheres of American life are largely dependent on cybernetic systems, their position as world leaders is explained by many things, as well as their interest in the issue of cyber security. In recent years, in addition to work within the framework of the North Atlantic Treaty Organization, the United States has developed active bilateral cooperation in the field of cyber security with many countries of the world[6].

The main directions of international cooperation on issues of ensuring cyber security

In general, international cooperation offers measures to ensure cyber security, which can be combined in the following key areas:

1. Regulatory and legal support:

1.1. Development of an international legal framework in the field of cyber security.

1.2. Coordination and harmonization of national laws of different countries in the field of cyber security.

1.3. Bringing it into line with the existing international legal norms of legislation in the field of cyber security, etc.

2. Technical and procedural measures:

2.1. Development of mechanisms and procedures for the interaction of various structures at all levels.

2.2. Development of unified protocols and security standards.

2.3. Authorization of hardware and software authentication schemes.

2.4. Creation of a universal digital identification system.

3. Creation and coordination of the activities of the organizational structure to ensure cyber security:

3.1. Formation of organizational structures responsible for the development of policies in the field of cyber security, monitoring, notification and response to incidents in cyberspace.

3.2. Training and coordination of the created organizational structure.

4. Staff training in the field of cyber security:

4.1. Assisting in the training of personnel for the organizational structure of cyber security.

4.2. Staff training according to a unified training program.

5. Coordination of activities of international cooperation participants:

5.1. Creation of an international coordinating body on cyber security issues.

5.2. We constantly share best practices in cyber security at various levels.

5.3. The direction of development of international cyber security systems in the direction corresponding to the evolution of challenges in this area [7].

[6] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

[7] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

Normative, technical, procedural and organizational measures should be implemented at the national and regional levels, but they should be coordinated at the international level. The last 2 areas of international cooperation in the field of cyber security will pass through all the previous 3 areas.

The main measures of international cooperation in the field of cyber security and communication between them are as follows:

1. Legal actions. Development of international legislation in the field of cyber security. Harmonization of national laws. Bringing it into line with the existing international legal norms of legislation in the field of cyber security.

2. Technical and procedural measures. Development of mechanisms and procedures for the interaction of various structures at all levels. Development of unified protocols and security standards. Authorization of hardware and software authentication schemes.

3. Organizational structure. Formation of an organizational structure responsible for security in cyberspace. Training and coordination of the created organizational structure.

4. Coordination of activities. Creation of an international coordinating body on cyber security issues. Constant exchange of best practices. Development directions of international cyber security systems.

5. Staff training. Assisting in the training of personnel for the organizational structure of cyber security. Staff training according to a unified training program.

Thus, the formation of the cyber security sector at the international and national levels is still ongoing. This process faces many challenges due to the innovative nature of cybersecurity issues. Currently, active efforts are being made to establish international cooperation on cyber security issues in various forms. The main directions of such cooperation are the development of a regulatory and legal framework, technical and procedural foundations of cyber security, creation of organizational structures, training of personnel and coordination of actions of interested parties. At the same time, considerable attention is paid to taking into account existing national and regional initiatives in order to avoid duplication of functions[8].

It is important to note that when developing cyber technologies for defense, each country relies on its internal needs and its own strategic approach. Ukraine can study the current practices and technologies of different countries, adapt them to its needs and develop appropriate capabilities of cyber warfare to ensure national security. Given the experience and practice of developing cyber technologies in these countries, it is important for Ukraine to develop its own strategic approach that will meet the needs and threats of the country, which will allow strengthening its defense cyber capabilities, using every positive element. In general, Ukraine can adopt the aggressive practices and technologies of other countries to develop its own cyber-technical capabilities in the field of security and defense.

A general overview of indicators that will allow financing the development of the defense sector and the cyber technology industry throughout the country (Fig. 1) reveals the attitude of these countries to the priorities of the development of cyber technologies and the attitude of national leaders to this industry.

The cost of developing cyber technologies in the field of defense can vary depending on the selected funding prospects in a given year and from country to country. It depends on many factors: the geopolitical situation, the presence of cyber security threats, the country's strategic plan. The development of cyber technologies in the field of defense is an urgent task

[8] Danyk Yu.G. Fundamentals of cyber security and cyber defense (Odessa: ONAZ named after O.S. Popova, 2019), 320.

for many countries, since these technologies are becoming an increasingly important component of modern military strategy[9].

The main characteristics of cyber security of the EU countries

For the European Union, cyber security policy acquired a comprehensive strategic aspect quite late. In 2001, the European Commission published the first document outlining the EU's approach to information security: "Network and Information Security: A European Policy Approach"[10]. Attacks on information systems can have serious consequences on a national scale, including the failure of communication systems and the leakage of confidential information. In early 2004, the European Union Network and Information Security Agency (ENISA) was established, which actively cooperates with Europol, the European Center for Combating Cybercrime and other specialized EU institutions.

The practical formation of the Autonomous Cyber Policy of the EU began only after the Cyber Security Strategy was approved in February 2013, and the document itself has the title: "Cyber Security Strategy of the European Union: Open and Secure Cyberspace." Since then, intensive development of the EU policy in the field of cyberspace has begun in all dimensions: the digital economy; networks and information security; fight against cybercrime[11]. This mainly concerns EU cooperation with NATO and other security services.

In particular, in 2016, Brexit and the uncertainty about the future of transatlantic relations after the election of Donald Trump as the US president intensified discussions about expanding strategic autonomy and strengthening the independence of the EU in the field of security and defense. Thus, the global strategy of the European Union's foreign and security policy, adopted in 2016, reflects the evolution of the Association's approach to cyber security. Recognizing that information technologies have become the basis for the functioning and well-being of European society, the EU considers that cyber security is one of its main security priorities[12]. In 2016, the following EU directive "On measures with a high level of general security of networks and information systems on the territory of the Union" was adopted, which forms uniform rules and requirements in the field of cyber security of the member states.

The main threats to national cyberspace in EU member states include:

a) providing state support or knowledge to other states and companies for the purpose of obtaining state or industrial secrets, personal data or other valuable information that may adversely affect the level of cyber security;

b) using the Internet for terrorist purposes (for propaganda, financing or recruiting supporters);

c) cybercrime (theft of personal data and laundering of illegally obtained funds).

Based on the results of data analysis for the period from 2019 to 2023, the EU cybersecurity agency presented a list of the 15 main types of cyberattacks (in order of

[9] Lester Evans. (2020). Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners. Independently published. P. 240.

[10] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Network and Information Security: Proposal for a European Policy Approach. COM(2001)298 final. Brussels, 6.6.2001. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF

[11] Challenges to effective EU cybersecurity policy Briefing Paper March 2019. European Union, 2019. 72 p.

[12] Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. June 2016. Brussels, 2016. 56 p.

quantitative detection from those that occur more often)[13]. Among the targets of cyberattacks, the EU Cybersecurity Agency singles out representatives of organized crime (57% of the number of cyberattacks), the state (12%), insiders (11%), system administrators (10%), users (7%) and others (3%)[14]. Such data testify to the systematic and repetitive nature of the organization and execution of cybercrimes at the international level.

The national legislation of the country, as a rule, provides for the protection of personal data (Netherlands, Estonia, Sweden, Finland, Spain), protection of e-commerce and security of electronic transactions and means of payment (Poland, Estonia, Italy, France)[15]. The cyber strategies of many European countries allow not only defensive, but also aggressive behavior in cyberspace.

Despite the obvious achievements of recent years, the EU policy in the field of cyber security still remains problematic. First of all, it lacks the necessary adjustments, this is obvious both at the regulatory and institutional level. The EU faces the problem of a shortage of qualified specialists in the field of ICT, especially in the field of cyber security. In the traditional dimension (so-called "hard power"), the full strategic autonomy of the EU, associated with the availability of its own cyber defense capabilities, has not yet been realized. EU member states recognize the need to strengthen their resources, but do not want to share their capabilities and developments. In addition, the capabilities of individual states are very diverse. In the field of cyber defense, European countries prefer cooperation and division of tasks between the EU and NATO, but the actions of the EU are considered to be largely complementary.

The EU still lags far behind the US in cyber security funding, mainly from world leaders. The total cost of cyber security in the EU as a percentage of GDP is about 0.1%. In the United States, the figure for 2023 was 0.41% (including the private sector)[16]. Although cybersecurity spending is not easily separated from total government budget spending, previous studies have shown that its level in Europe (as a percentage of GDP) is low and suboptimal compared to other global players, mainly the United States.

At the EU level, investments in cyber security are made within the framework of various joint budget programs. In the period 2014-2020, within the framework of the Horizon 2020 program, about 6 billion euros were invested in projects on cyber security and the fight against cybercrime. The European Structural Investment Funds (ESI) provide annual contributions of approximately €4 billion for targeted activities and investments in cybersecurity. In the period 2014-2017, about 30 million euros were invested from the Connecting Europe Fund. By comparison, in the United States, in 2017 alone, the government allocated more than $19 billion from the budget to Ensure Cybersecurity Policy[17].

At the same time, the main problem is not that Europe cannot innovate or lacks infrastructure, but that the main weakness is still the creation of big brands. There is not a single

[13] The year in review. From January 2019 to April 2020. ENISA Threat Landscape. 2020. 24 p.
[14] Main incidents in the EU and worldwide. From January 2019 to April 2020. ENISA Threat Landscape. 2020. 25 p.
[15] Zakonodavstvo ta strategii y sferi kiberbezpeky krayin Yevropeyskogo Soyuzu, SSHA, Kanady та inshyh. Informatsiyina dovidka, pidgotovlena Yevropeyskym informatsiyino-doslidnytskym tsentrom na zapyt narodnogo deputata Ukrayiny. Kyiv: Infotsentr, Yevropeyskyy informatsiyno-doslidnytskyy tsentr, Laboratoriya zakonodavchyh initsiatyvs, 2016. 37 p.
[16] Challenges to effective EU cybersecurity policy Briefing Paper March 2019. European Union, 2019. 72 p.
[17] Cybersecurity. State of federal it report. Public release version 1.0. Policy Papers. URL: https://www.cio.gov/assets/resources/sofit/02.05. cybersecurity.pdf

Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

European company among the world's 10 largest internet companies, computer equipment manufacturers and ICT companies.

The main focus in the EU structure is on the issue of organizational and managerial support for cyber security, the development of protection systems, and similar imbalances in the system of financing certain areas of cyber policy against cyber attacks are one of the main reasons for the weakness of the EU's position in the world, the international cyber security system is dominated by the USA and China.

Cooperation between NATO and the EU in the field of cyber defense is developing almost continuously and is not politicized. The implementation of the Joint Declaration of NATO and the EU, signed at the Alliance summit in Warsaw in 2016, is progressing harmoniously in the field of cyber security. Since the EU pays special attention to the so-called "soft security", the development and financing of the following areas of activity are primarily carried out here:

a) strengthening the external aspect of the EU policy in the field of cyber security;

b) increasing the resilience of ICT networks and systems to cyber threats;

c) development of capabilities and tools for responding to cyberattacks, effective cooperation in the fight against cybercrime;

d) promotion of standards and values in cyberspace. The development of these industries will determine the potential of the EU in the field of cyber security and its position on the world stage. However, in the coming years, Member States will need to take coordinated action based on information, supported by appropriate levels of funding[18].

The emergence of new cyber threats mentioned in national and international policy, the need to expand the scope of application of cyber security rules within the EU itself became the reason for further improvement of the legal framework of the EU cyber policy, in particular, the development of a draft of the new EU cyber security strategy, published publicly in December 2020. A week prior to this event, the European Agency for Scams, which, among other things, was involved in the certification of vaccines against COVID-19, announced a cyber attack. The document provides for a regime of sanctions for certain countries that threaten EU cyber security (in particular, Russia, China, North Korea, etc. are recognized as such), strengthens cyber intelligence, creates a joint energy and military cyber security structure within the framework of permanent structural cooperation in the EU (PESCO). , and promotes cooperation between Western Balkan countries, Eastern partners, etc. The European Union has created a project to combat cybercrime in the southern regions of the EU. In addition to the previously approved areas of internal EU cybersecurity rules (health care, banking, drinking water supply, energy infrastructure), the European Commission proposes to add the administrative area, food sector and pharmaceutical production[19]. Thus, the EU acts in accordance with the requirements of the times and tries to adequately respond to new challenges and threats in the field of cyber security.

An example of the development of the PESCO mechanism mentioned in the framework of the cyber security policy is the EU Rapid Response Team for Cyber Attacks (CRRT), which was created in 2020 with the participation of representatives of 6 European

[18] Communication from the Commission to the European Parlament, the Council, the European Economic and Social Committee and the Committee of the Regions 2030 Digital Compass: the European way for the Digital Decade//COM/2021/118 final// https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118.

[19] Joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.9.2017. JOIN(2017) 450 final. URL: https://eur-lex. europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450

countries[20]. An international rapid response team is on standby in multiple locations and is ready to respond immediately in the event of a cyber attack. The results of this pilot international project should be spread throughout the European Union and become the basis for multinational EU cyber armies.

The main characteristics of cyber security of NATO countries

In NATO countries, cyber defense is a key aspect of the renewal of the North Atlantic Alliance and its adaptation to new threats. After a new Strategic Concept was adopted at the Lisbon Summit in November 2010, NATO's cyber defense policy was approved in June 2011 and "enhanced" at the Newport (Wales) Summit in September 2014. In the conditions of rapid development of the Internet and IoT (Internet of Things), attacks are becoming more and more sophisticated, which makes it difficult to predict and respond to them. Thus, France has created one of the most successful systems for combating cybercrime, as it devotes a lot of attention, effort and resources to adopting world experience and applying it to itself. It is important to note that such a serious system and such important security measures do not limit the basic rights of citizens, organizations and mass media. Currently, there is no complete system of protection against all possible cyber threats, but France is confidently developing its own cyber defense, this allows it to conduct internal and external policies without unnecessary threats and maintain a leading position in solving global challenges.

NATO is considered the most influential international organization that has modernized information security policy, which defines cyber security as the main priority of its activities, taking into account its understanding of cyberspace as an environment for conducting information warfare. The organization established NATO's advanced center in member states as a multinational organization that develops cyber security doctrines, improves interstate cooperation, implements theoretical developments in the field of countering cyber threats, shares cyber defense experience of experts from member countries and partners, and introduces methods of countering cyber threats. Currently, the NATO Cyber Security Center operates in Estonia. The creation of the center was carried out precisely at the initiative of the Estonian authorities and the first sponsor country, which signed a memorandum of understanding regarding the center's activities and accreditation. It should be emphasized that the center is not a unit of the military command or a NATO force structure, personnel and financial resources are provided by the sponsoring and participating countries[21].

At the same time, the organization's documents say that, as cyber threats to NATO's security become more frequent, complex, more disruptive and coercive, NATO leadership, member states and allies rely on collective cyber defense to fulfill the Alliance's core missions and operational crisis management. Thus, cyber security has become one of the main priorities of the transatlantic organization due to the fact that hybrid attacks can cause damage to the military and civilian spheres of life of the participating countries, so the measures approved in the last few years will contribute to the effective protection of NATO against cyber threats. In the 2019 regulations, changes were made to the main principles of cyber security of the Alliance, which confirm the following: cyber security is considered as a component related to the main task of NATO collective defense, the principles of international law are applied to

[20] Shaping Europe's digital future. Policy. Cybersecurity. European Commission. URL: https://ec.europa.eu/digital-single-market/en/cybersecurity
[21] NATO Cooperative Cyber Defence Centre (CCDCOE). URL: https://www.cybersecurityintelligence.com/ nato-cooperative-cyber-defence-centre-ccdcoe-395.html

Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

cyberspace, and cyber security is aimed at protecting the organization's own network and increasing its defense capabilities.

The main characteristics of cyber security of the BRICS association

Cooperation of the BRICS Association in the field of international security is carried out within the framework of annual summits, informal meetings of the heads of state and government of the participating countries, protocol meetings of high representatives on national security issues and working groups on international information security. As stated in the official documents of the organization, the strengthening of cooperation in the field of information security shows that the issue of combating new high-tech weapons depends not only on the actions of international and national institutions, including the joint task of ensuring information security, but also on the coordination of security policy and international cooperation on on a multilateral basis. In previous years, the BRICS information security strategy was based on the project of the Russian Federation and the UN Group of Experts on the implementation of the Russian proposal in the document on international information security, while other Russian proposals were rejected by the BRICS countries and always voted "against".

At the same time, the rapid progress of information and communication technologies in the BRICS countries, especially in China and India, has led to a significant modernization of the Association's policy in the field of information security, which consists in recognizing the importance of ensuring cyber security and information sovereignty of the country. Studies show that in order to protect information sovereignty, the BRICS countries are developing laws on information sovereignty, taking into account the provisions on new data protection standards, their confidentiality and the introduction of tools to limit the access of foreign technology companies to the domestic cyber environment. As noted by high-ranking officials of the BRICS member states, complete trust in foreign technologies affects the protection of personal data, the threat of manipulation of collective consciousness and critically important state systems.

The governments of the BRICS countries also noted that the large-scale use of Internet services and social networking platforms by citizens of the Association is a sign of the country's political system, which invests heavily in programs to digitize the economy and industry against hacker attacks, given that strict cyber security standards are the key to protection against hacker attacks attacks and intellectual potential of each BRICS country. On the other hand, it should be noted that this may threaten national security. In particular, we are talking about India's insistence on storing personal data of its citizens only on the country's computer resources, the adoption of the law on information sovereignty in Russia, the approval of a new general law on data protection in 2018, the computerization of government operations and the introduction of IoT for industrial automation in Brazil. In addition, according to the organization's experts, the BRICS countries are the countries where the majority of cyberattacks occur simultaneously, and the countries where cyberattacks occur most often. The current situation puts the issue of cyber security at the forefront of the agenda of the BRICS member states[22].

The new program of action of the informal organization "From BRICS to CyberBRICS: New cooperation in the field of cyber security" was discussed at the ministerial meeting on communication development of the BRICS countries, held in Brazil in August 2019. During the meeting, a joint declaration was adopted, which emphasizes the strategic interests

[22] Belli L. BRICS countries to build digital sovereignty. URL: https://www.opendemocracy.net/en/hri-2/ brics-countries-build-digital-sovereignty/

of the BRICS partnership in the field of new digital infrastructure, 5G and IoT technology, as well as cyber security. Officials confirmed that modern infrastructure, effective cyber security management and, in particular, the establishment of data protection standards are important resources for the comprehensive and sustainable development of the BRICS countries. Digital transformation at the political level of BRICS is recognized as an important component of the economic and social future of the participating countries, therefore the development and implementation of digitalization strategies that affect the competitiveness of the Union countries at the international level can be carried out in various areas, from traditional digital technologies to intellectual, and precisely with the use of artificial intelligence and robotic technologies, which determine the long-term development potential of the organization's participants. This line of activity is aimed at creating new opportunities for cooperation between the BRICS countries in the region.

At the same time, it was noted that China is indeed the country that follows the most systematic approach to technological innovation and has invested heavily in 5G technology. For example, China has adopted laws on cyber security, e-commerce and data protection standards that meet international standards. Instead, Brazil only recently launched its annual digital transformation strategy, which government agencies are working to develop but have no cybersecurity provisions. In such a difficult situation, it can be argued that digital transformation can bring great benefits and create great risks.

Experts note that the large number of interconnected devices controlled through 5G networks can significantly improve robotics, industrial automation and intelligent agriculture, as well as provide significant efficiency gains through powerful data collection and processing capabilities. It also takes into account the fact that half of the BRICS population is already connected to the Internet and generates an incredible amount of data. In fact, such advances, as the researchers emphasize, not only revolutionize online and offline activity and provide unprecedented opportunities, but also create new multifaceted threats, this is due to the fact that the interconnection of IoT requires the highest level of security to avoid hacking , data leaks and turning digital expectations of the BRICS countries into potential problems.

The new action program also raises questions about the need for joint cooperation and comparative views on information security policy in the BRICS countries. This is important not only for mutual understanding and respect for each country's position, but also for the development of compatible technologies and regulations that facilitate access to innovative services and products while protecting users' rights. The BRICS countries may take different positions in terms of the sensitivity and vulnerability of specific issues, but their priorities and goals are very similar in basic thinking. In this context, an effective multi-stage approach allows BRICS governments to interact with academics, representatives of the private sector and civil society and receive information and answers on various aspects of cybersecurity policy. The implementation of the initiative on the cooperation of interested parties will be a useful strategy for all members of the Association.

First, the governments of the BRICS member states, which in recent years have consistently emphasized the importance of strengthening cooperation in the field of scientific research and technology development, can support the creation of a cooperation mechanism of the BRICS analytical center on cyber security issues. As the pioneering experience of the CyberBRICS project shows, the analysis of existing digital policies is of paramount importance to identify best practices and propose sustainable and equitable solutions. According to the member states of the organization, the presidency of Brazil in BRICS alternately with other countries provided a unique opportunity to formulate an active and innovative Agenda,

Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

emphasizing the benefits of improving cooperation in the field of digital policy in general and cyber security in particular. Thus, the priority of the cooperation of the BRICS countries in the field of information security is to increase the effectiveness of the fight against new types of high-tech weapons and ensure information security[23].

The main characteristics of cyber security in Japan

Japan is one of the most advanced information countries in the world, and to maintain its reputation, it must ensure a decent level of cyber security. The range of groups affected by cyberattacks, from individuals and families to companies engaged in complex social infrastructure, is rapidly expanding. Despite the best efforts of the Japanese government, the risk of information attacks is increasing. This risk affects areas such as national security, risk management, and the competitiveness of the Japanese economy.

Japanese industry lags behind American and European industry in assessing cyber threats. According to government statistics for the year 2023, only 65% of Japanese companies conduct a cyber security risk assessment, compared to about 85% of such companies in the US and 75% in Europe.

In June 2013, the Information Security Policy Council adopted the Cyber Security Strategy. The Japanese government uses the term "information security" in its policies and major plans. However, with the growing number of cyber threats that go beyond information security, such as creating obstacles to the operation of public life support facilities, Tokyo decided to use the term "cyber security" for the first time to address all these issues.

The strategy is aimed at creating a world-leading, stable and dynamic cyberspace and turning Japan into a world leader in the field of cyber security. To achieve these goals, the document outlines four main principles:

- ensuring free exchange of information;
- proposals for new measures to respond to the growing risk;
- appropriate measures to counter cyber threats based on risk assessment;
- taking measures, based on one's own social responsibility, and interaction with other countries.

The state body that regulates relations in the field of cyber security is the National Information Security Center (NISC), which develops draft state standards for information security measures, develops recommendations based on the results of the assessment of the state of cyber security, and promotes the implementation of measures to improve the state of cyber security.

The main characteristics of China's cyber security

China is vulnerable because it does not have a single unified cyber defense strategy. The main tasks in the field of cyber defense are set by the Chinese government:

1. Protection of cyberspace sovereignty;
2. Protection of critical information infrastructure (ICI);
3. Creating a healthy online culture;
4. Fight against cybercrime, espionage and terrorism;
5. Improvement of cyberspace management;
6. Major improvements in the field of cyber security;

[23] From BRICS to CyberBRICS: New Cybersecurity Cooperation. URL: http://www.chinatoday.com.cn/ctenglish/2018/tpxw/201911/t20191113_800184922.html

7. Increasing the ability to protect cyberspace;
8. Strengthening international cooperation [24].

Over the past years, China will continue to manage information and technology through the CSL and related regulations. All companies operating in China require data localization, especially for "critical" data. Regulators are also looking to use technologies (such as encryption) that meet security and manageability requirements[25].

Enforcement measures are largely based on regulatory documents in which they have adopted regulatory policies to protect China's cyberspace and core areas countering the activities of hostile groups[26].

Key features of UK cyber security

It is well known that Great Britain is a country that keeps its secrets very carefully. This can be explained, in particular, by the history of the public key cryptographic system. Her algorithm was first developed and published in 1977 by MIT scientists Ronald Raivest, Adi Shamir, and Leonard Adleman. The lead in solving this task belongs to British scientists Clifford Cox and Malcolm Williamson, who did it in 1973, but until 1997 the algorithm itself and its use were classified[27].

Modern cyber defense systems require highly qualified personnel, which the relevant special services are looking for among various population groups. NCSC has developed a strong recruitment system, so that anyone studying applied technology, mathematics or language in the organization is given the opportunity to participate in real projects.

The CyberFirst program is a major part of the government's national program. It encompasses a wide range of activities, scholarship programs, summer schools, and more, and it offers a complete package of financial support and cyber skills training for talented entry-level students and applicants under the leadership of NCSC.

A detailed analysis of closed and active programs shows that their target audience is getting younger every year. The most surprising thing is that some of the proposals now apply to young people who graduated from school in 2020-2023, but there is a condition that these individuals have to do well in STEM subjects.

In particular, people with special needs can apply to work in the GCHQ system, but the immediate environment, British citizenship and residency requirements have been unchallenged for most of the past 10 years.

"To disclose or not to disclose" - under such an eloquent title, a post was published on the website of the department (GCHQ and the relevant structural units of the NCSC) in November 2018. As with other materials, the UK's national security interests are best served by the accumulation of knowledge rather than its publication.

There are 2 ways to address vulnerabilities in cyberspace. The first is to identify and address this vulnerability for the benefit of technology users worldwide. The second way is to preserve knowledge of this vulnerability and use it for intelligence purposes in the future, and

[24] China publishes first national cybersecurity-strategy [Електронний ресурс]. –Режим доступу: http://www.usito.org/news/china-publishes-first-national-cybersecurity-strategy.
[25] Cyberspace Administration of China [Електронний ресурс]. –Режим доступу: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm
[26] China's Cyber Security Law: how prepared are you? [Електронний ресурс]. –Режим доступу: https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law.
[27] Welcome to GCHQ.Pioneering a new kind of security for an ever more complex world [Електронний ресурс]. –Режим доступу: www.gchq.gov.uk.

to stop the activities of people who seek to harm the security of the UK[28]. The decision to support 1 of these approaches was made by a group of world-leading experts from three agencies (GCHQ, NCSC and the Ministry of Defence).

The high level of work of the National Cyber Security Center of Great Britain is indicated by the fact that this unit was created by Microsoft as part of the Microsoft Bug Bounty program in the first quarter of 2018[29].

Britain, as a self-sufficient sovereign state, has its own standards, from the design of road signs, the measurement of length in miles and yards, pint milk bottles and some electrical outlets to more serious issues of livelihood. At the same time, this does not make the country undesirable for various types of cooperation, rather, on the contrary, it arouses great respect and interest, and protection against cyber attacks should be at a fairly high level.

The main characteristics of cyber security of Ukraine: problems and prospects

The cyber security strategy of Ukraine defines the priorities of national interests in the field of cyber security, existing and potentially possible cyber threats to create conditions for the safe functioning of cyber space, goals and objectives for ensuring cyber security in Ukraine, its use for the benefit of individuals, society and the state.

The strategy determines that ensuring cyber security is one of the priorities of the national security system of Ukraine. Implementation of this priority will be achieved by strengthening the capacity of national cyber security systems to counter cyber threats in the modern security environment.

It should be noted that cyberspace, along with other physical spaces, is perceived as one of the theaters of possible military operations, at the same time, there is a growing tendency to create cyber armies, which not only protect critical information infrastructure from cyber attacks, but also provide for preventive attacks in cyberspace.

The Russian Federation still remains one of the main causes of threats to national and international cyber security, this country is actively implementing the concept of information warfare, based on a combination of destructive actions and informational and psychological manipulations in cyberspace, the mechanism of which is actively used in the hybrid war against Ukraine.

In the future, interstate confrontation and an increase in the intensity of intelligence and subversive activities in cyberspace are predicted. The circle of states that are trying to form their own cyber intelligence, master modern technologies of intelligence and destructive activities in cyberspace, and strengthen state control over the national segment of the Internet is expanding. At the same time, these tools are widespread, and the tendency to carry out reconnaissance and destructive activities in cyberspace is increasing, mainly due to the involvement of special services of the Russian Federation, international hacker groups in carrying out cyber attacks. The strategy also draws attention to the growing use of cyberspace by terrorist organizations on a global scale.

The strategy defines the main challenges and threats for Ukraine in the field of cyber security:

- active use of cyber tools in international competition;

[28] Equities process Publication of the UK's process for how we handle vulnerabilities.[Електронний ресурс]. – Режим доступу: www.ncsc.gov.uk/blog-post/equities-process.

[29] A new approach for cyber security in the UK (2016). Retrieved from: https://www.ncsc.gov.uk/news/new-approach-cyber-security-uk.

- the competitive nature of the development of cyber security tools in the context of rapid and progressive changes in information and communication technologies, especially in cloud and quantum computing, 5G networks, big data, IoT, artificial intelligence, etc.;

- the militarization of cyberspace and the development of cyberweapons allow covert cyberattacks to be carried out in support of combat operations, intelligence operations and sabotage operations in cyberspace;

- the impact of the COVID-19 pandemic and the full-scale invasion of February 24, 2022 on economic activity and social behavior led to the fact that significant segments of public relations are still able to work remotely with the wide use of electronic services and information and communication systems;

- introduction of innovative technologies from the point of view of cyber security measures, new technologies of electronic interaction between citizens and the state, digital services that are provided without proper risk assessment[30].、

In addition to the main subjects of the National Cyber Security System, Ukraine includes business entities, public organizations and individual citizens of Ukraine, while issues in the field of National Coordination of the Cyber Security Center play a rather important unifying and coordinating role in this process.

The main priorities for ensuring cyber security in Ukraine, especially in the face of a full-scale invasion, have been determined:

- provision of cyberspace for the protection of national sovereignty and social development;

- protection of the rights, freedoms and legitimate interests of Ukrainian citizens in cyberspace;

- integration of Europe and Euro-Atlantic in the field of cyber security. The formation of a new quality of the national cyber security system requires a clear and understandable definition of strategic goals that must be achieved during the implementation of this strategy.

To build a deterrence system (C), it is necessary to achieve the following strategic goals:

Purpose C.1. Effective cyber protection;

Purpose C.2. Effective countering intelligence and sabotage in cyberspace and cyberterrorism;

Purpose C.3. Effective fight against cybercrime;

Purpose C.4. Development of asymmetric deterrence tools.

To achieve cyber resilience (K), it is necessary to achieve the following strategic goals:

Purpose K.1. National preparedness for cyberspace and reliable cyber defense;

Goal K.2. professional development, scientific and technical support of a cyber-aware society and cyber security;

Goal K.3. Secure digital services.

To improve interaction (B), it is necessary to achieve the following strategic goals:

Purpose B.1. Strengthening the cooperation system;

Goal B.2. Formation of a new model of relations in the field of cyber security;

[30] Cyber security in Ukraine: ways of development and opportunities [Electronic resource] URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

Goal B.3. Practical international cooperation[31].

The strategy also determines the direction of Ukraine's foreign policy activities in the field of cyber security.

In the field of cyber security, Ukraine should unify the approaches, methods and means of ensuring cyber security with the established practices of the EU and NATO, strengthen the cyber resilience of Ukraine, develop the capabilities of national cyber security systems and protect national interests in cyberspace. On the part of the government of Ukraine, deepening of the process of European integration should be ensured by adopting other measures agreed with key foreign partners aimed at strengthening the process of European integration.

The coordinator of the implementation of this strategy is the National Cyber Security Coordination Center, a working body of the National Security and Defense Council of Ukraine.

The strategy is implemented directly by the main participants of the National Cyber Security System, the Ministry of Foreign Affairs of Ukraine, the Ministry of Digital Transformation of Ukraine, the Ministry of Education and Science of Ukraine and other structures dealing with cyber security issues, within the limits of their capabilities and powers.

Funding of measures to implement the strategy is provided at the expense of the State Budget of Ukraine and from other sources that are not prohibited by law.

This strategy is based on the Constitution of Ukraine, the Laws of Ukraine "On the National Security of Ukraine" and "On the Basic Principles of Ensuring Cybersecurity in Ukraine", the Convention on the Protection of Human Rights and Fundamental Freedoms, the Convention on Combating Cybercrime, the National Security Strategy of Ukraine, the Concept of Countering Terrorism in of Ukraine and other legal acts.

Conclusion

Europe is interested in the comprehensive development of EU policy in the field of cyber security. The cross-border nature of cyber threats leads to the fact that the stability of the EU in this matter directly affects the security of EU member states. The current direction of the EU's potential development and especially close cooperation with NATO make it possible to avoid complex political dilemmas. The Euro-Atlantic community is interested in preventing the fragmentation of cyberspace and preserving its open, free and universal character in the face of today's complex challenges to international security, in particular the spread of cybercrime of all kinds. According to the official data of the cyber security agency of the European Union, among the list of types of cyber attacks, the number of privacy violations is increasing, this problem determines the need to develop a system for the protection of human rights in the field of cyber security and joint activities in solving this problem on the part of all EU member states. One of its fundamental elements is the need to update legislation, especially in accordance with the new EU cyber security strategy.

The transformation of the information paradigm of global development, which reflects the new regularities of the formation of the modern system of international relations, proves the innovativeness of international cooperation in the field of information and communications and, accordingly, requires the improvement of policies to ensure international peace and stability. The modernization of the information security policy of international organizations is determined by the ability of international relations officials to ensure multilateral dialogue, to take into account the different positions of global governance officials to counter the latest

[31] Cyber security in Ukraine: ways of development and opportunities [Electronic resource] URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html

Eximia Journal
Vol. 14, 1-20, January, 2025
ISSN: 2784-0735
www.eximiajournal.com

information threats, and to act in accordance with their legal authority as a universal international platform to reach consensus on solving problems that related to security issues.

Increasing cyber security and reducing the number of cyber attacks in cyberspace should become the main topic of discussion in today's world. This problem must be solved as soon as possible, because the created samples of cyber weapons are characterized by global coverage, almost instantaneous impact, without the possibility of receiving warnings about their use. Cyber protection is the only means that can prevent the loss of information in the security sphere of both Ukraine and other countries and the interference of some countries in internal affairs. During the analysis of the state of cyber security in the developed countries of the world, the main areas of protection against cyber threats, protection of the sovereignty of cyber space in the largest countries of the world and national security of Ukraine were determined.

Appendices

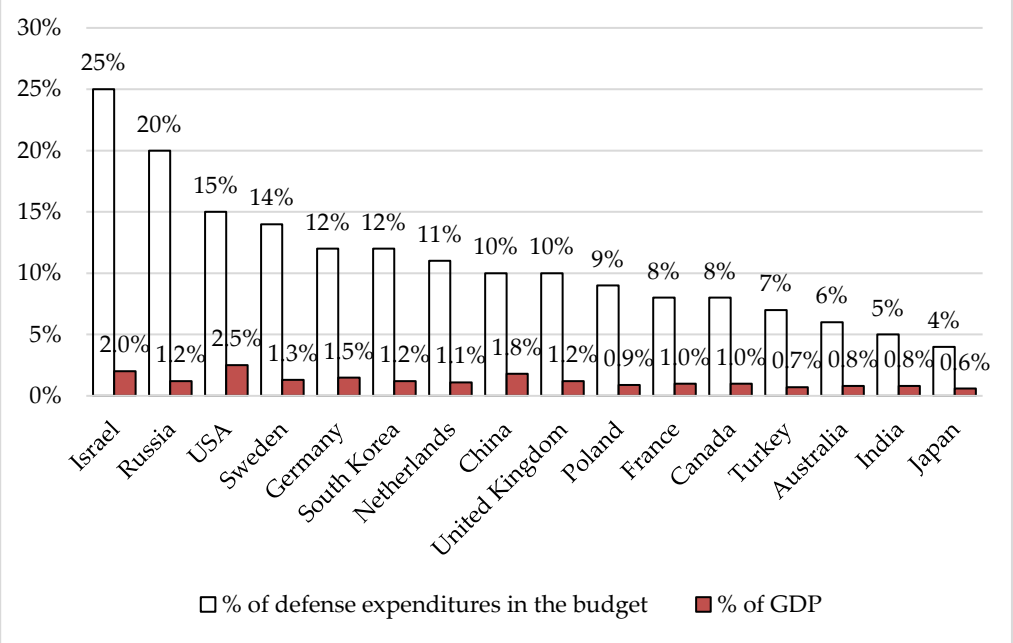

Figure 1. Average share of spending on cyber technologies from GDP and in the defense budget of some countries of the world (2018-2023)
Source: compiled by the author on the basis of annual reports of the countries of the world