EVROPSKÝ POLITICKÝ A PRÁVNÍ DISKURZ

Svazek 9

3. vydání

2022

●

EUROPEAN POLITICAL AND LAW DISCOURSE

Volume 9

Issue 3

2022

DOI: 10.46340/eppd.2022.9.3

Přístup redakce

Evropský politický a právní diskurz – mezinárodní časopis věnovaný mezinárodnímu právu, vnitřním právním předpisům evropských zemí, politologie, mezinárodním vztahům. Pro publikaci v časopisu přijímají se vysoce kvalitní články, což představují důležité inovativní, teoretické, koncepční, metodické a empirické příspěvky v příslušných oborech vědy.

V časopisu se uplatn´uje systém anonymního recenzování pro ověření kvality vědeckých článků.

Evropský politický a právní diskurz má velký zájem zejména o interdisciplinární výzkumy v oblasti politologie a právní vědy, jsou to srovnávací analýzy nebo prozkoumání jednotlivých jevů. Zároveň vítáme jakékolív výzkumy týkající se politických a právních problémů různých národních a mezinárodních institucí. Evropský politický a právní diskurz přijímá k publikaci jenom původní materiály a nebere v úvahu možnost zveřejňovat dříve tištěné članky.

Editorial Policy

The *European Political and Law Discourse* – international Journal of International Law, domestic Law of European countries, Political Science, Social Communications, International Relations, Sociology is a peer reviewed journal with blind referee system, which aims at publishing high quality articles that may bring innovative and significant theoretical, conceptual, methodological and empirical contributions to the fields.

The *European Political and Law Discourse* has a particular interest in interdisciplinary approaches to law, political science, social communications and sociology, whether through comparative or single case-study analysis, but by no means restricts its interests to these spaces, welcoming any relevant contribution from and about different parts of the World.

The *European Political and Law Discourse* accepts original articles which are not under consideration elsewhere at the time of submission.

The Journal is indexing by Index Copernicus:
https://journals.indexcopernicus.com/search/details?id=42760

EVROPSKÝ POLITICKÝ A PRÁVNÍ DISKURZ
Evidenční číslo: MK ČR E 22311
Vydavatel: BEROSTAV DRUŽSTVO
Adresa: Vlastislavova 562/15, 140 00, Praha 4 – Nusle

Table of contents

INTERNATIONAL LAW AND INTERNATIONAL RELATIONS

MEDIA DIMENSIONS OF SOCIAL AND POLITICAL DISCOURSE

CONTEMPORARY PROBLEMS OF NATIONAL PUBLIC AND PRIVATE LAW

CONTEMPORARY PROBLEMS OF NATIONAL PUBLIC AND PRIVATE LAW

DOI: 10.46340/eppd.2022.9.3.3

Andrii Pravdiuk, PhD in Law
ORCID ID: https://orcid.org/0000-0002-5248-8111
Vinnytsia National Agrarian University, Ukraine

THE STATE AND CURRENT ISSUES OF LEGAL REGULATION OF CYBER SECURITY IN UKRAINE

The article studies urgent issues of the legal regulation of cyber security in Ukraine in view of current challenges. It is stated that under conditions of intensification of cyberattacks on the information and telecommunication systems of the state authorities of Ukraine, computer networks need reliable protection. It was determined that cyberattack and cyberterrorism are negative phenomena that cause social crises, so research and analysis of Ukrainian legislation on cybersecurity is extremely important and necessary. Due to the rapid growth of cyber risks and cyber threats, it is important to monitor the current state of cybersecurity in our country, highlight the main problems of building a national cyber defense system and identify areas for their solution. This requires an analysis of the measures that have been implemented in the field of protection of computer and telecommunications networks from cyberattacks, as well as the definition of measures needed to be implemented to create conditions for the safe operation of cyberspace. The study reveals significant political, economic and social efforts aimed to strengthen cyber resilience, which the state is making to develop national cybersecurity capabilities. Considering the purpose and objectives of the scientific article, the authors have studied in detail the legal aspect. As a result of scientific research, it has been established that the legal regulation of cyber security in Ukraine is carried out by normative acts of various legal force: the Constitution of Ukraine, laws and regulations of Ukraine. The Constitution of Ukraine contains initial provisions on the organization of security of both the national cyberspace as a whole and the virtual space of public authorities of Ukraine, which are reflected in the laws as well as normative and legal regulations of Ukraine. Analysis of the current legislation in the field of cyber security has revealed some of its imperfections. It has been found that effective cybersecurity needs to be addressed comprehensively and requires coordinated action at the national, regional and international levels to prevent, prepare, and respond to the incidents by the government, the private sector and civil society.

Keywords: cybersecurity, information law, information security, cyberspace, information society, cyber protection, cyber defense.

Relevance of research. Nowadays, the issue of the national security of the state is becoming extremely important due to the intensification of external security threats, increasing pressure in the field of economy, information policy, technology, etc. Together with the internal problems experienced by the state (imbalance of reform processes, etc.), this situation requires systematic comprehensive efforts to neutralize these threats, especially in the information environment. It is the information space and resources, information technology and infrastructure that have the greatest impact on solving these problems.

Current realities show that cyber threats are evolving at the accelerated pace, cybercrime is becoming more sophisticated, better organized and transnational. This is caused by the fact that the Internet, digital services, information and communication technologies (ICTs) have become an integral part of the global economy, from e-document management, online shopping, and online banking to the Internet of things and smart systems of the enterprise management. While the dependence on ICT use in business and entrepreneurship is growing, cyber risks and cyber threats are also increasing, which requires early response to prevent or address them and awareness of the risk factors of all stakeholders[1]. Hence, the security of national cyberspace, which requires the introduction of the latest technological advances, as well as the administrative efficiency of the state and the private sector, is fundamental to the implementation of our strategy. A technocratic approach to cyberspace alone is not enough to solve problems that arise. Broad tools for effective coercive measures need to be developed to prevent possible escalation and to contain deterrence from hostile structures. On the other hand, educational work should continue on an ongoing basis[2].

Analysis of recent research and publications shows that the problem of legal regulation of cybersecurity has been studied by I. V. Diorditsa, V. A. Lipkan, E. A. Tymoshenko, A. L. Pravdiuk, B. A. Kormych, I. P. Kushnir, Yu.E. Maksymenko, M.A. Strelbitskyi, O.K. Yudina and others. However, despite a large number of publications on this issue, the state and legal regulation of cybersecurity in Ukraine still requires further research.

The purpose and objectives of the scientific article is to study the current state of legal regulation of cybersecurity in Ukraine and identify current issues that need to be addressed.

Presentation of materials. The growth of modern society is closely related to the prevention of various threats that increase during the reform of any sphere of society[3]. Professor Oleksandr Korystin argues that the issue of combating hybrid threats in the information sphere, in particular in cyberspace, covers the problems of the national security quite widely and comprehensively. This, above all, requires a substantial analysis of the situation, the study of factors that cause inability to respond effectively in order to counter hybrid threats, in particular the rights and freedoms of citizens and the interests of society and the state.

In addition, the objectivity and validity of the research results requires an appropriate methodological framework, acceptability of the data used in the analysis, and the sources which they come from. Today, under conditions of information society development, cybernetic security, or cybersecurity, is a necessary and important condition for the functioning and development of the information society. Given the constant integration and globalization processes in the world, the leading states of the world are already paying much more attention to the issues of the search for protection and countering cyber threats, both internal and external. For this purpose, there are being developed national cybersecurity systems that can bring together many systems, authorities and the private sector to combat such threats[4].

In 2013, the European Union adopted the Cyber Security Strategy targeted at the open, reliable and secure cyberspace. It includes measures to achieve cyber resilience, significantly reduce cybercrime, develop a cyber defense policy related to the Common Security and Defense Policy, develop production and technological resources for cybersecurity, create a coherent international cyberspace policy for the EU and promote EU core values. Immediately after the publication of the Strategy, the work on the relevant directive was started. It is important to emphasize that this document was developed not separately from other areas, but as part of the Digital Single Market Strategy, on the one hand, and part of the European Agenda on Security, on the other. Both the Strategy and Agenda were published in the spring of 2015. In July 2016 the European Commission presented “Additional measures on promoting the cybersecurity industry development”, and on July 6, 2016 the EU Directive on the measures aimed to ensure a high overall level of security of the network and information systems throughout the European Union was adopted[5].

Cybersecurity is a strategic issue of the national importance, among the EU member states cybersecurity strategies have been adopted by Sweden (2008), Estonia (2008), Finland (2008), Slovakia (2008), Czech Republic (2011), France (2011), Germany (2011), Lithuania (2011), Luxembourg (2011),

[1] Трофименко,О., Прокоп, Ю., Логінова, Н., Задерейко, О. (2019). Кібербезпека України: аналіз сучасного стану. *Захист інформації, 21 (3),* 150-157. DOI: 10.18372/24107840/21/13951.

[2] Тарасюк, А. В. (2021). Теоретико-правові основи забезпечення кібербезпеки України*: автореферат дисертації доктора юридичних наук*. Київ: Національний авіаційний університет.

[3] Користіна, О. Є. (ред.) (2015). *Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні.* Київ: Скіф.

[4] Кондратюк, М. В.(2019). Кібербезпека України в системі національної безпеки. *Право і суспільство, 6 (2),* 42-48. DOI: https://doi.org/10.32842/2078-3736-2019-6-2-7.

[5] European Union Website (2017). *An Open, Safe and Secure Cyberspace* <http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf> (2022, April, 11).

and the Netherlands (2011). The list of countries clearly shows that the problem of cybersecurity is recognized worldwide as an important one. In particular, Estonia is one of the European leaders in the field of cybersecurity and the NATO Cyber Security Center is located in Tallinn. On November 25, 2016, during the visit of the Center, President Kersti Kaljulaid claimed, "There is no doubt that cyberspace as a battlefield can be compared to the sea, air and water"[1].

In particular, 27 NATO member states, the European Union (EU), 12 non-NATO European countries and 38 other countries have currently adopted national cybersecurity strategies. It can be stated that in 2022 Ukraine joined the cyber center at NATO, which enables to exchange experience in the field of cyber security between Ukraine and other member states of the center. Being located in Tallinn, CCDCOE is a NATO-accredited cybersecurity and analytical center specializing in interdisciplinary applied research, analysis, information exchange, and cybersecurity training[2].

Nowadays, the EU has faced a shortage of qualified ICT professionals and especially cybersecurity experts. The proposal of the EU budget for 2021-2027 emphasizes the development of digital skills, especially in the field of cybersecurity. The European Commission has invested more than € 63.5 million in four pilot projects to lay the groundwork for a European network of cybersecurity expertise centers to strengthen cybersecurity research and coordination in the EU. Four pilots, CONCORDIA, ECHO, SPARTA and CyberSec4Europe, are aimed at contributing to the Joint European Roadmap for Cyber Security and Innovation since 2020 and the European Cyber Security Strategy for Industry. In addition, they will assist the EU in identifying and testing management models for the European network of experts in the field of advanced cybersecurity technology centers[3].

It is worth noting that in Ukraine the issue of training specialists in the field of cybersecurity is also quite urgent. Accelerating the pace of technological development of society has led to a significant lag of higher education from the growing demands of the market, both in the field of information technology and cybersecurity. Accessibility, level and quality of education, along with indicators such as GDP per capita and life expectancy are one of the three internationally accepted indicators of the Human Development Index in the annual UN assessment of life quality in the world[4].

Ukrainian universities train specialists in specialty 125 Cybersecurity, but in different specializations with the focus on cybersecurity management, on the legal aspects, and on the technical training. In our University there has been selected the way of training within the specialty standard in order to provide enhanced training in programming. The inclusion of courses on ethical hacking will be a logical continuation of training specialists who are good at programming. Such coordination will, firstly, raise the level of training in Ukraine through the international cooperation, and secondly, combat cybercrime together with experts from different countries, because, unlike real space, cyberspace has no state borders[5]. In its turn, in modern conditions, training in cybersecurity cannot be limited to obtaining higher education in the educational institution in the relevant specialty. Competitiveness and professionalism must be constantly increased on the basis of the "concept of lifelong learning", the multiplicity of forms and methods of which opens another promising area for the intersectoral cybersecurity public and private partnership. There are several options for activities in this direction, including postgraduate training in cybersecurity-related specialties, the use of nonlinear training, the use of potential non-formal education to improve the skills of practitioners through cyber-training, seminars, international internships, etc[6]. The need

[1] Lawtrend – Исследования Образование Действия (2022). *Кибербезопасность: рекомендации для ЕС* <http://www.lawtrend.org/in formation-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es> (2022, April, 11).

[2] Українська правда (2022). *Україна приєдналася до кіберцентру при НАТО – крок, який раніше блокувала Угорщина* <https://www.pravda.com.ua/news/2022/03/5/7328456/> (2022, April, 11).

[3] Lawtrend – Исследования Образование Действия (2022). *Кибербезопасность: рекомендации для ЕС* <http://www.lawtrend.org/in formation-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es> (2022, April, 11).

[4] Куценко, В. І. (2011). Перспективи розвитку системи підготовки кадрів : пошук альтернативи. *Ефективна економіка*, 1.

[5] Пашорін, В. І. (2019). Термінологічні та освітні аспекти кібербезпеки. *Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукраїнської науково-практичної конференції (Київ, 27 березня 2019 р.)* Київ: Київський національно торгово-економічний університет.

[6] Дубов, Д. (2018). Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України. *Аналітична доповідь. Національний інститут стратегічних досліджень.* Київ.

for further development of the system of training in the field of cybersecurity is also evidenced by the regulations that have been recently adopted by the Government that are aimed at ensuring the functioning of the national cybersecurity system. Thus, in December 2021, the Regulations on the Organizational and Technical Model of Cyber Defense were approved (Resolution of the Cabinet of Ministers of Ukraine of December 29, 2021 No 1426[1].

In Ukraine, legal regulation of cybersecurity measures was mainly determined by the requirements of Euro-Atlantic integration and stemmed from the doctrines, strategies and guidelines of NATO and the EU, so it is advisable to analyze the state of regulation at the level of strategic planning documents in Ukraine's national security[2]. According to Article 25 of the Law of Ukraine "On the National Security of Ukraine"[3], the purpose of planning in the areas of the national security and defense is to ensure implementation of the state policy in these areas by developing strategies, concepts, programs, plans for security and defense, resource management and efficient allocation. These documents are mandatory and the basis for the development of specific programs by the components of the state national security policy.

In Ukraine, cybersecurity is considered as a component of the national security. The Cyber Security Strategy of Ukraine was approved by the Decree of the President of Ukraine of December 30, 2021[4]. This Strategy is based on the provisions of the Convention on Cybercrime, ratified by the Law of Ukraine of September 7, 2005 No 2824-IV[5], legislation on the national security, legislation on domestic and foreign policy, electronic communications, protection of the state information resources and other protected information, as well as aimed at implementation by 2022. The National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine on May 26, 2015 No 287 "On the decision of the National Security and Defense Council of Ukraine of May 6, 2015 "On the National Security Strategy of Ukraine". The Cyber Security Strategy of Ukraine approved by the Decree of the President of Ukraine on March 15, 2016[6], the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine", adopted on October 5, 2017, laid down the general principles of building the national cybersecurity system, and defined the main tasks and competencies of cybersecurity actors.

The Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine", adopted on October 5, 2017, laid down the general principles of building a national cybersecurity system, as well as defined the main tasks and competencies of cybersecurity actors.

According to Article 1 of the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" of October 5, 2017, protection of information in cyberspace is nothing but a set of organizational, legal, engineering and technical measures, as well as measures of cryptographic and technical protection of information aimed at preventing cyber incidents, detection and protection against cyberattacks, elimination of their consequences, restoration of stability and reliability of functioning of communication, technological systems[7].

Cybercrime is not limited to crimes committed on the global Internet. It applies to all types of crimes committed in the information and telecommunications sphere, where information, information resources, information technology can be the subject (purpose) of criminal encroachments, the environment in which offenses are committed, and the means or instrument of crime. This approach is more successful and

[1] *Постанова про затвердження Положення про організаційно-технічну модель кіберзахисту, 2021* (Кабінет Міністрів України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text> (2022, April, 11).

[2] Довгань, О., Доронін, І. (2017). Розвиток законодавства у сфері кібербезпеки: інформаційно правове дослідження. *Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Економіка і право, 32*, 91-101.

[3] *Закон України Про національну безпеку України, 2021* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (2022, April, 11).

[4] *Стратегія кібербезпеки України, 2022* (Президент України). *Офіційний сайт Президента України* <https://www.president.gov.ua/documents/372022-41289> (2022, April, 11).

[5] *Закон України Про ратифікацію Конвенції про кіберзлочинність, 2005* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/994_575> (2022, April, 11).

[6] *Стратегія кібербезпеки України, 2022* (Президент України). *Офіційний сайт Президента України* <https://www.president.gov.ua/documents/372022-41289> (2022, April, 11).

[7] *Закон України Про основні засади забезпечення кібербезпеки України, 2017* (Верховна Рада України) *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2163-19> (2022, April, 11).

reasonable in terms of the nature of cyberspace, which is formed by all possible local and global information and telecommunications networks, although the Internet is predominant among them[1]. In general, according to certain characteristics and features of the sphere of distribution and influence, cybercrime can be characterized as an economic, political and discriminatory offense, which manifests itself in various forms, including illegal political struggle, financial fraud, etc.; in the form of information, the dissemination of which is potentially harmful as it relates to, for example, illicit trafficking in weapons, explosives, explosive devices, their manufacture, trafficking in human beings, human organs, drugs, psychotropic substances, prescriptions for their production, etc[2].

Information security is a well-developed branch of science and technology that offers a wide range of different means of data protection. However, no single tool provides the required level of protection for information systems. Protection (security) at the required level is possible only if comprehensive complementary measures are taken, namely normative and legal ones, administrative ones, special equipment and software[3].

The use of the Internet and information technology opens up endless possibilities for humanity, as well as causes new serious threats. More and more information is moving online, and according to the latest estimates, there are already more than 20 billion devices connected to the Internet in the world, which is several times more than the population of the Earth. Billions of gigabytes of various information are also collected on servers. The world is becoming open, and such rapid growth requires the formation of “game rules”[4]. Cyberspace has become a very important part of modern life. It solves many social problems, has a great impact on the economy and innovation, etc. Due to this, cyberspace is very promising for the development, and at the same time it is the main target for attackers. Cyberattacks on information infrastructure have become a real threat, and countering these attacks is one of the main challenges for risk management.

Having defined cyberspace as a new habitat of modern man, its key characteristics should be specified. One of such characteristics is its virtuality. Modern use of the concept of “virtuality” goes beyond the field of computer science and computer technology. The terms “virtual corporation”, “virtual money”, “virtual democracy”, “virtual learning”, etc., which seemed to be unrealistic until recently, have entered everyday life. Thus, virtual reality is becoming as objective as possible, extremely specific and tangible. Virtuality is not the opposite of reality. However, virtuality means that something in cyberspace may not be what it seems to be[5]. Thus, cyberspace, being a virtual place, is not a place in the usual sense when the place or space for interaction is limited by the space and time frames.

The cross-border nature of cyberspace, its dependence on complex information technologies, active use of cyberspace sites and services by all segments of the population identify new opportunities, but also cause new threats, including: a) harm to the rights, interests and lives of individuals, organizations, government agencies; b) cyberattacks against information resources by cybercriminals and cyberterrorists; c) the use of cyber weapons in war and cyber wars, including those that accompany traditional hostilities[6].

Despite all public calls for the peaceful use of cyberspace in the interests of all people and nations, the governments of the same countries that are calling for this have actively joined the cyber-disarmament race, reproducing the classic “security dilemma” on a qualitatively new basis. This means that against the background of complex and contradictory global processes of political, economic and social development,

[1] Веселова, С. Ю. (2021) Адміністративно-правові основи кібербезпеки в умовах гібридної війни: *дисертація на здобуття наукового ступеня доктора юридичних наук.* Одеса: Одеський Державний Університет Внутрішніх Справ.

[2] Довгань, О. Д., Доронін, І. М.(2017). *Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту*. Київ: АртЕк.

[3] Ромашко, С. М. (2007). *Опорний конспект лекцій з дисципліни "Інформаційні системи в менеджменті"* <http://www.dut.edu.ua/uploads/l_1937_18003221.pdf> (2022, April, 11).

[4] Сліпченко, Т. (2020). Кібербезпека як складова сисеми захисту національної безпеки6: європейський досвід. *Актуальні проблеми правознавства, 1 (21).* DOI: 10.35774/app2020.01.128.

[5] Гайдук, О. В. (2019). Кіберпростір як площадка та інструмент вппливу на соціально-економічні процеси. *Безпека соціально-економічних процесів в кіберпросторі: матеріали Всеукраїнської науково-практичної конференції* (Київ, 27 березня 2019 р.) Київ : Київський національно торговельно-економічни університет.

[6] Павленко, В. С. (2021). Сутність кібербезпеки у теорії інформаційного права. *Право та державне управління, 2,* 28-33. DOI: https://doi.org/10.32840/pdu.2021.2.4.

cyberspace is becoming a space of the Cold War v 2.0, i.e. the basis of a new confrontation of key geopolitical actors, which will take place mainly in cyberspace[1].

During the war, the Internet is becoming a powerful weapon, which is significantly enhanced by artificial intelligence technologies. Cyber weapons include a wide range of technical and software tools, which are often aimed at the use of vulnerabilities in data transmission systems[2].

It is worth recalling that the countries of the North Atlantic Alliance refer cyberattacks to the main modern hybrid threats. Cyberspace is an operational zone of hostilities on a par with land, sea and air. Cyber defense is recognized as an important element of collective defense ("cyberattack may lead to the application of the provision on collective defense (Article 5 of the NATO Treaty)"[3].

Since 2020, 5G technology has been introduced, which could lead to a faster and more expanded network of IoT devices. This innovation has immediately led to major DDoS attacks and new cybersecurity challenges. A characteristic trend in the field of modern cyber threats is software upgrades. The main threat is that unprotected vulnerabilities are a major cause of systemic trade-offs. Support for Windows 7 ended on January 14, 2020, leading to more unsupported and unprotected obsolete systems and, as a result, there may be prone to attacks, as was the case with the WannaCry ransomware attack, which has plagued many organizations for irregular operating system updates and the use of obsolete and unsupported operating systems such as Windows XP (and soon this may be Windows 7)[4].

In Ukraine, the majority of incidents involve the distribution of malicious software to the public sector. According to the State Special Communications Service, during mid-February and early March, Ukrainian organizations suffered about 2,800 cyberattacks, and the historical record for the day in Ukraine was 271 DDoS attacks. Thus, to be compared: there were 2,200 cyberattacks in 2021. Their number has increased 5 times over the last three years. Top 5 cyberattacks of the 21st century confirm the importance of cybersecurity of business of any size and domain in the information society. As reported by Microsoft, since October 2021, 19% of cyberattacks in the world have been directed against Ukraine. It ranks the second after the United States. In its turn, 98% of all cyberattacks use a human factor and are intended for untrained users and business management[5].

According to the latest research, the percentage of computers infected with malware in Ukraine is one of the highest in the world and amounts to 28.7%, i.e. one in three computers is infected with malware. Under such conditions, it is extremely important to use a set of software and hardware that would ensure an acceptable level of infrastructure security, namely: effective and reliable antivirus software, intrusion prevention systems, internetwork screens, modules for the device control and Internet access, systems for data encryption, mobile device management, protection of mail servers and collaboration systems, etc. Regular intrusion testing and configuration verification (on your own or with the help of external organizations) will allow you to detect configuration errors before hackers gain access to the user's server or computer[6].

Current ability to access everything connected to the Internet is a luxury we can't afford to lose. However, the more people use online systems, the more cyber threats they have. One of the most vulnerable places of the virtual world is a mobile phone with access to social networks, messengers, and dozens of mobile applications, often of unknown origin, where people easily share private information that, at first glance, is not critical[7].

It should be noted that a large part of Ukrainian society neglects the calls of the military, and in particular the Ministry of Defense of Ukraine, which clearly warns on its official website and notes that

[1] Дубов, Д. (2014). *Кіберпростір як новий вимір геополітичного суперництва*. Київ: НІСД.

[2] Біленчук, П., Кулик, В. (2018). Стратегія забезпечення кібербезпеки в гібридній війні. *Lexinform* <https://lexinform.com.ua/dumka-eksperta/strategiya-zabezpechennyakiberbezpeky-v-gibrydnij-vijni/> (2022, April, 11).

[3] NATO (2022). *Колективна оборона – Стаття 5* <https://www.nato.int/cps/uk/natohq/topics_110496.htm> (2022, April, 11).

[4] Пікус, Р. В., Бабенко, Ю. Л.(2022). Кіберстрахування: нові можливості для страхового ринку України. *Економіка та держава, 2,* 134-140. DOI: 10.32702/2306-6806.2022.2.134.

[5] Підгайна, Є. (2022). Кібербезпека для бізнесу під час війни: як завадити шкідливому трафіку, фішинговим атакам, зараженню вірусами та іншим загрозам. *Mind* <https://mind.ua/publications/20238234-kiberbezpeka-dlya-biznesu-pid-chas-vijni-yak-zavaditi-shkidlivomu-trafiku-fishingovim-atakam-zarazhennyu> (2022, April, 11).

[6] Bischoff, P. (2021). "Which countries have the worst (and best) cybersecurity?" *Comparitech* <https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/> (2022, April, 11).

[7] Аушев, Є. (2020).Безпека в інтернеті: найпростіші правила захисту даних. *Сайт BBC News Україна* <https://www.bbc.com/ukrainian/blogs-51444737> (2022, April, 11).

social networks give the website administration the opportunity to collect information about personal data without the knowledge of the individuals as it is impossible to track collection of relevant information in such systems. Posting photos on the social network page with weapons or military equipment, providing information about the location of even one soldier can lead to the loss of an entire unit[1], photos of the movement of military units of the Armed Forces of Ukraine have been published and unfortunately continue to be published. Therefore, in our opinion, though with a very long delay as it should have been done in 2014, Ukraine passed the law No 2160-IX, which introduced criminal liability for taking photos and videos of the movement of the Ukrainian military. It has to supplement the Criminal Code of Ukraine with a new Article 114-2 "Unauthorized Dissemination of Information on the Sending, Transfer of International Military Assistance to Ukraine, Movement, Transfer or Deployment of the Armed Forces of Ukraine or Other Military Units of Ukraine Committed in Martial Law or State of Emergency"[2].

The results show that the consistent development of the legal framework in 2016-2022 and the development of a cyber defense strategy for 2021-2025 have had a positive impact on the institution building and detection of cybercrime in Ukraine. Building cooperation with developed countries (USA) has helped to fight cybercrime by facilitating US law enforcement investigations. This means that international experience is effective for developing countries as a way to quickly understand the threats and risks of cybercrime[3].

In addition to the positive dynamics of development of legislation in the field of cybersecurity, it should be noted that it is necessary to harmonize national legislation with the international standards. In particular, the legislation of Ukraine does not provide definitions of such terms as "user of services", "data on the movement of information" and "electronic evidence" and does not regulate "urgent storage of computer data stored", "urgent storage and partial disclosure of data on the information flow", which hinders effective implementation of provisions of the Budapest Convention and limits the possibilities of mutual assistance with other countries in the field of cybercrime prevention and combating cybercrime[4]. We share the opinion of scientists who argue that it is necessary to improve public administration in the security and defense sector, including the systems for cybersecurity, information protection and security of information resources; it is important to strengthen the capabilities of intelligence and counterintelligence bodies by creating organizational, logistical and financial conditions for concentrating their operational capabilities on the priority areas of operational and service activities, strengthening the capacity of cybersecurity actors to effectively combat cyber threats of military nature, cyberespionage, cyberterrorism and cybercrime, strengthening the institutional and technical capabilities of such entities, deepening international cooperation in this area[5].

Conclusions. In times of war, the problem of guaranteeing information security through the spread of various types of cyber threats becomes a matter of the national security, the issue of every citizen and society as a whole, so it is a strategic problem of the state that requires a comprehensive system to support cybersecurity and information sovereignty, establish strategic communication of the subjects of the national cybersecurity system, build capabilities to counter cyber threats, form appropriate infrastructure of the domestic information space. The legislator is obliged to pursue a policy of anticipation and immediate response to the dynamic changes taking place in cyberspace, to develop and implement effective

[1] Офіційний веб сайт Міністерства оборони України (2016). *Правила інформаційної та кібернетичної безпеки в зоні проведення АТО* <https://www.mil.gov.ua/ukbs/pravila-informaczijnoi-ta-kibernetichnoi-bezpeki-v-zoni-provedennya-ato.html> (2022, April, 11).

[2] *Закон України Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану, 2022* (Верховна Рада України). *Офіційний сайт Верховної Ради України* <https://zakon.rada.gov.ua/laws/show/2160-%D0%86%D0%A5#Text> (2022, April, 11).

[3] Pravdiuk, A., Gerasymenko, I., Tykhonova, O. (2021). Overcoming Cybercrime in Ukraine (Cyberterrorism). *IJCSNS International Journal of Computer Science and Network Security, 21 (6),* 181-186.

[4] Тарасюк, А. В.(2020). Пріорітети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник, 1(30),* 133-136. DOI: https://doi.org/10.32837/pyuv.v0i1(30).532. (2022, April, 11).

[5] Грібоєдов, С.М. (2021). Удосконалення державного планування у сфері забезпечення кібербезпеки в умовах гібридних загроз. *Інформація та право, 1(36),*114-122.

means and tools of possible response to aggression in cyberspace, which can be used as a means of deterring military conflicts and threats in cyberspace.

Under conditions of globalization of cyber threats, it is reasonable to unify approaches to legal regulation in the field of cybersecurity and standardize security measures for effective cooperation and coordination of efforts at the national and international levels.

Aspirations of Ukraine for the European integration oblige to improve national legislation in the field of cybersecurity, taking into account the terms of the Association Agreement between Ukraine, on the one hand, and the EU and Member States, on the other. Implementing the experience and best practices of EU countries and NATO standards should be a priority. It should be noted that the problem of effective cybersecurity will be solved only through the coordinated action at the national, regional and international levels, so in our opinion it is an indisputable fact that today laws must meet the requirements of the modern level of technology development.

References:

1. Trofymenko,O., Prokop, Yu., Lohinova, N., Zadereyko, O. (2019). Kiberbezpeka Ukrayiny: analiz suchasnoho stanu [Cybersecurity of Ukraine: analysis of the current state]. *Zakhyst informatsiyi* [Information protection], *21 (3),* 150-157. DOI: 10.18372/24107840/21/13951 [in Ukrainian].
2. Tarasyuk, A. V. (2021). Theoretical and legal bases of cybersecurity of Ukraine [Theoretical and legal bases of cybersecurity of Ukraine]: *abstract of the dissertation of the doctor of legal sciences* [abstract of the dissertation of the doctor of legal sciences]. Kyiv: National Aviation University. [in Ukrainian].
3. Korystin, O.Ye. (eds.) (2015). *Protydia vidmyvaniu koshtiv: mizhnarodni standarty, zarubizhnyi dosvid, administratyvno-pravovi, kryminolohichni, kryminalno-pravovi, kryminalistychni zasady ta systema finansovoho monitorynhu v Ukraini* [Anti-money laundering: international standards, foreign experience, administrative-legal, criminological, criminal-law, forensic principles and the system of financial monitoring in Ukraine]. Kyiv: Skif. [in Ukrainian].
4. Kovalchuk, T, Korystin, O., Svyrydiuk, N.(2019). Hibrydni zahrozy u sektori tsyvilnoi bezpeky v Ukraini [Hybrid threats in the civil security sector in Ukraine.]. *Nauka i pravookhoronna* [Science and law enforcement], *3 (45),* 69-79. DOI: https://doi.org/10.36486/np. [in Ukrainian].
5. Kondratiuk, M. (2019). Kiberbezpeka Ukrainy v systemi natsionalnoi bezpeky[Cybersecurity of Ukraine in the national security system]. *Pravo i suspilstvo* [Law and society], *6 (2),* 42-48. DOI https://doi.org/10.32842/2078-3736-2019-6-2-7. [in Ukrainian].
6. European Union Websites (2017). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* <http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf> (2022, April, 11).
7. Lawtrend – Issledovaniya Obrazovaniye Deystviya (2022) [Lawtrend – Research Education Action (2022)]. *Kiberbezopasnost: rekomendatsii dlya YeS* [Cybersecurity: Recommendations for the EU] <http://www.lawtrend.org/in formation-access/blog-information-access/kiberbezopasnost-rekomendatsii-dlya-es> (2022, April, 11). [in Russian].
8. Lohinova, N. I. (2016). Pravovi osnovy kiberbezpeky v Ukraini [Legal bases of cybersecurity in Ukraine]. *Pravovi ta instytutsiini mekhanizmy zabezpechennia rozvytku derzhavy ta prav v umovakh yevrointehratsii* [Legal and institutional mechanisms for ensuring state and rights development in the conditions of European integration: Proceedings from the International Scientific and Practical Conference], 1, 575-577. [in Ukrainian].
9. Ukrayinska pravda (2022) [Ukrainian Truth (2022)]. *Ukrayina pryyednalasya do kibertsentru pry NATO – krok, yakyy ranishe blokuvala Uhorshchyna* [Ukraine has joined NATO's cyber center, a move previously blocked by Hungary] <https://www.pravda.com.ua/news/2022/03/5/7328456/> (2022, April, 11). [in Ukrainian]
10. Kutsenko, V. I. (2011). Perspektyvy rozvytku systemy pidhotovky kadriv: poshuk alternatyvy [Prospects for the development of the training system: finding an alternative]. *Efektyvna ekonomika* [Efficient economy], *1.* [in Ukrainian].
11. Pashorin, V. I. (2019). Terminolohichni ta osvitni aspekty kiberbezpeky [Terminological and educational aspects of cybersecurity]. *Bezpeka sotsialno-ekonomichnykh protsesiv v kiberprostori: materialy Vseukrayinskoyi naukovo-praktychnoyi konferentsiyi (Kyiv, 27 bereznya 2019 r.)* [Security of socio-economic processes in cyberspace: materials of the All-Ukrainian scientific-practical conference (Kyiv, March 27, 2019)]. Kyiv: Kyiv National University of Trade and Economics, 28-30. [in Ukrainian].
12. Dubov, D. (2018). *Derzhavno pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy* [Public Private Partnership in Cybersecurity: International Experience and Opportunities for Ukraine]. Kyiv: NISD. [in Ukrainian].
13. *Postanova pro zatverdzhennya Polozhennya pro orhanizatsiyno-tekhnichnu model' kiberzakhystu, 2021* (Kabinet Ministriv Ukrayiny) [Resolution on approval of the Regulation on the organizational and technical model of cyber defense, 2021 (Cabinet of Ministers of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny*

[Official site of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/ 1426-2021-%D0%BF#Text> (2022, April, 11). [in Ukrainian].

14. Dovhan, O., Doronin, I. (2017). Rozvytok zakonodavstva u sferi kiberbezpeky: informatsiino pravove doslidzhennia [Development of cybersecurity legislation: information and legal research]. *Naukovyy chasopys Natsionalnoho pedahohichnoho universytetu imeni M.P. Drahomanov. Ekonomika i pravo* [Scientific Journal of the National Pedagogical University named after MP Dragomanov. Economics and law], *32*, 91-101. [in Ukrainian].
15. *Zakon Ukrayiny Pro natsionalnu bezpeku Ukrayiny, 2021* (Verkhovna Rada Ukrayiny) [Law of Ukraine on National Security of Ukraine, 2021 (Verkhovna Rada of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny* [Official site of the Verkhovna Rada of Ukraine] <http://zakon.rada.gov.ua/ laws/show/2429-19> (2022, April, 11). [in Ukrainian].
16. *Stratehiya kiberbezpeky Ukrayiny, 2022* (Prezydent Ukrayiny) [Cybersecurity Strategy of Ukraine, 2022 (President of Ukraine)]. *Ofitsiynyy sayt Prezydenta Ukrayiny* [Official site of the President of Ukraine] <https://www.president.gov.ua/documents/372022-41289> (2022, April, 11). [in Ukrainian].
17. *Zakon Ukrayiny Pro ratyfikatsiyu Konventsiyi pro kiberzlochynnist, 2005* (Verkhovna Rada Ukrayiny) [Law of Ukraine on Ratification of the Cybercrime Convention, 2005 (Verkhovna Rada of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny* [Official site of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua> (2022, April, 11). [in Ukrainian].
18. *Zakon Ukrayiny Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny, 2017* (Verkhovna Rada Ukrayiny). *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny* [Official site of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/2163-19> (2022, April, 11). [in Ukrainian].
19. Veselova, S. Yu. (2021). Administratyvno-pravovi osnovy kiberbezpeky v umovakh hibrydnoyi viyny [Administrative and legal bases of cybersecurity in the conditions of hybrid war]: *dysertatsiya na zdobuttya naukovoho stupenya doktora yurydychnykh nauk* [the dissertation on competition of a scientific degree of the doctor of legal sciences]. Odesa: Odessa State University of Internal Affairs [in Ukrainian].
20. Dovgan, O. D., Doronin, I. M. (2017). *Eskalatsiya kiberzahroz natsionalnym interesam Ukrayiny ta pravovi aspekty kiberzakhystu* [Escalation of cyber threats to the national interests of Ukraine and legal aspects of cyber defense]. Kyiv: ArtEk. [in Ukrainian].
21. Romashko, S. (2007). *Opornyi konspekt lektsii z dystsypliny "Informatsiini systemy v menedzhmenti"* [Reference syllabus of lectures on the subject "Information Systems in Management"] <http://www.dut.edu.ua/uploads/l_1937_18003221.pdf> (2022, April, 11). [in Ukrainian].
22. Slipchenko, T. (2020). Kiberbezpeka yak skladova systemy zakhystu natsionalnoi bezpeky: yevropeiskyi dosvid [Cybersecurity as a component of the national security protection system: European experience]. *Aktualni problemy pravoznavstva, 1 (21).* DOI: 10.35774/app2020.01.128> (2022, April, 11). [in Ukrainian].
23. Haiduk, O. (2019). Kiberprostir yak ploshchadka ta instrument vpplyvu na sotsialno-ekonomichni protsesy [Cyberspace as a platform and tool for influencing socio-economic processes]. *Bezpeka sotsialno-ekonomichnykh protsesiv v kiberprostori: materialy Vseukrayinkoyi naukovo-praktychnoyi konferentsiyi (Kyiv, 27 bereznya 2019 r.)* [Security of socio-economic processes in cyberspace: materials of the All-Ukrainian scientific-practical conference (Kyiv, March 27, 2019)]. Kyiv: Kyiv National University of Trade and Economics, 28-30). [in Ukrainian].
24. Pavlenko, V. (2021) Sutnist kiberbezpeky u teorii informatsiinoho prava [The essence of cybersecurity in the theory of information law]. *Pravo ta derzhavne upravlinnia* [Law and public administration], 2, 28-33. DOI: https://doi.org/10.32840/pdu.2021.2.4. [in Ukrainian].
25. Dubov, D. (2014) *Kiberprostir yak novyi vymir heopolitychnoho supernytstva: Monohrafiia [Cyberspace as a new dimension of geopolitical rivalry: monograph*] Kyiv: NISS.[in Ukrainian].
26. Bilenchuk, P., Kulyk, V. (2018). Stratehiia zabezpechennia kiberbezpeky v hibrydnii viini [Cybersecurity strategy in hybrid warfare]. *Lexinform* <https://lexinform.com.ua/dumka-eksperta/strategiya-zabezpechennyakiberbezpeky-v-gibrydnij-vijni/> (2022, April, 11). [in Ukrainian].
27. NATO (2022). *Kolektyvna oborona – Stattya 5* [Collective defense – Article 5] <https://www.nato.int/cps/uk/natohq/topics_110496.htm> [in Ukrainian].
28. Pikus, R., Babenko, Yu. (2022). Kiberstrakhuvannia: novi mozhlyvosti dlia strakhovoho rynku Ukrainy [Cyber insurance: new opportunities for the insurance market of Ukraine]. *Ekonomika ta derzhava* [Economy and state], 2, 134-140. DOI: 10.32702/2306-6806.2022.2.134. [in Ukrainian].
29. Pidhaina, E. (2022). Kiberbezpeka dlya biznesu pid chas viyny: yak zavadyty shkidlyvomu trafiku, fishynhovym atakam, zarazhennyu virusamy ta inshym zahrozam [Cybersecurity for business during the war: how to prevent harmful traffic, phishing attacks, virus infections and other threats]. *Mind* <https://mind.ua/publications/20238234-kiberbezpeka-dlya-biznesu-pid-chas-vijni-yak-zavaditi-shkidlivomu-trafiku-fishingovim-atakam-zarazhennyu> (2022, April, 11). [in Ukrainian].
30. Bischoff, P. (2021). "Which countries have the worst (and best) cybersecurity?" *Comparitech* <https://www.comparitech.com/blog/vpnprivacy/cybersecurity-by-country/> (2022, April, 11). [in English].
31. Aushev, E. (2020). Bezpeka v interneti: nayprostishi pravyla zakhystu danykh. [Internet security: the simplest rules of data protection]. *Sayt BBC News Ukrayina* [BBC News Ukraine website] <https://www.bbc.com/ukrainian/blogs-51444737> (2022, April, 11). [in Ukrainian].

32. Official website of the Ministry of Defense of Ukraine (2016). *Pravyla informatsiynoyi ta kibernetychnoyi bezpeky v zoni provedennya ATO* [Rules of information and cyber security in the area of anti-terrorist operation] <https://www.mil.gov.ua/ukbs/pravila-informaczijnoi-ta-kibernetichnoi-bezpeki-v-zoni-provedennya-ato.html> (2022, April, 11). [in Ukrainian].
33. *Zakon Ukrayiny Pro vnesennya zmin do Kryminalnoho ta Kryminalnoho protsesualnoho kodeksiv Ukrayiny shchodo zabezpechennya protydiyi nesanktsionovanomu poshyrennyu informatsiyi pro napravlennya, peremishchennya zbroyi, ozbroyennya ta boyovykh prypasiv v Ukrayinu, rukh, peremishchennya abo rozmishchennya Zbroynykh Syl Ukrayiny chy inshykh utvorenykh vidpovidno do zakoniv Ukrayiny viyskovykh formuvan, vchynenomu v umovakh voyennoho abo nadzvychaynoho stanu, 2022* (Verkhovna Rada Ukrayiny) [Law of Ukraine on Amendments to the Criminal and Criminal Procedure Codes of Ukraine to Counteract Unauthorized Dissemination of Information on Sending, Moving Weapons, Weapons and Ammunition to Ukraine, Movement, Movement or Deployment of the Armed Forces of Ukraine or Other Military Formations under martial law or state of emergency, 2022 (Verkhovna Rada of Ukraine)]. *Ofitsiynyy sayt Verkhovnoyi Rady Ukrayiny* [Official site of the Verkhovna Rada of Ukraine] <https://zakon.rada.gov.ua/laws/show/2160-%D0%86%D0%A5#Text> (2022, April, 11). [in Ukrainian].
34. Pravdiuk, A., Gerasymenko, I., Tykhonova, O. (2021). Overcoming Cybercrime in Ukraine (Cyberterrorism). *IJCSNS International Journal of Computer Science and Network Security, 21 (6),* 181-186.
35. Tarasiuk, A. (2020) Prioritety pravovoho zabezpechennia kiberbezpeky v Ukraini na suchasnomu etapi [Priorities of legal support of cybersecurity in Ukraine at the present stage.] *Prykarpatskyi yurydychnyi visnyk* [Prykarpattya Legal Bulletin],*1(30)*, 133-136. DOI https://doi.org/10.32837/pyuv.v0i1(30).532. [in Ukrainian].
36. Hriboyedov, S.M. (2021). Udoskonalennya derzhavnoho planuvannya u sferi zabezpechennya kiberbezpeky v umovakh hibrydnykh zahroz [Improving state planning in the field of cybersecurity in the context of hybrid threats]. *Informatsiya ta pravo* [Information and law], *1(36)*, 114-122. [in Ukrainian].