ISSN Print 2414-0287
ISSN Online 2707-8426

PROJECT MANAGEMENT AND FINANCIAL AND ECONOMIC SECURITY AMID GLOBALIZATION

UDC 004.056.5:005.521:347.77(477) DOI https://doi.org/10.26661/2414-0287-2020-1-45-25

PROBLEMS OF CYBERSECURITY AND WAYS OF OVERCOMING CYBERCRIME IN UKRAINE

Cherep O.H., *Nurlikhina G.B., Saenko M.V.

Zaporizhzhia National University
Ukraine, 69600, Zaporizhzhia, Zhukovsky str., 66

**Almaty University*
Republic of Kazakhstan, 050031, Almaty, 36 Aksay-3 micro region

maxsaen72@gmail.com

ORCID 0000-0002-3098-0105, 0000-0001-8718-6984, 0000-0003-1907-7000

Key words:
cybercrime, cybersecurity, offense, prevention, information security, transformation process.

It has been proven that threats to the information security (IS) of people, society and the state are becoming more dangerous, and the negative informational impact on the individual and public consciousness is becoming more significant. It has been determined that information threats are of particular concern to the child, as a subject of public relations, which requires special protection and care from the state and society. An analysis of the current state of security of the IS in Ukraine suggests that the child protection system in Ukraine remains ineffective and needs a major transformation in line with current challenges and threats in the information field. The expediency of using legal modelling in law-making and law-enforcement practice is substantiated, which allows to avoid negative influence on the child's consciousness. It is established that the IS, as a component of national security, requires the use of the whole set of monitoring and forecasting mechanisms, but has its specificity. First, the IS is one of the most technological security sectors, actively using modern information technologies. Second, the IS is considered in at least two aspects: technical (cyber security and cyberwarfare, etc.) and ideological (propaganda, etc.). Third, the monitoring data, conclusions and recommendations provided by the IS are the basis of forecasting throughout the national security sector. The features of information security forecasting directions in the context of the development of modern information technologies are considered. Issues of cyber security have been identified, and ways to tackle cybercrime have been suggested.

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА ШЛЯХИ ПОДОЛАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Череп О.Г., *Нурліхіна Г.Б., Саєнко М.В.

Запорізький національний університет
Україна, 69600, м. Запоріжжя, вул. Жуковського, 66

**Університет «Алмати»*
Республіка Казахстан, 050051, м. Алмати, 36 Аксай-3

Ключові слова:
кіберзлочинність, кібербезпека, правопорушення, запобігання, інформаційна безпека, трансформаційний процес.

Доведено, що загрози інформаційній безпеці (ІБ) людини, суспільства і держави стають все більш небезпечними, а негативний інформаційний вплив на індивідуальну та суспільну свідомість - дедалі суттєвішим. Визначено, що особливу небезпеку інформаційні загрози становлять для дитини як суб'єкта суспільних відносин, який потребує особливого захисту і піклування з боку держави та суспільства. Аналіз сучасного стану забезпечення ІБ в Україні дає підстави стверджувати, що система захисту дитини в Україні залишається недостатньо ефективною і потребує кардинальної трансформації відповідно до сучасних викликів і загроз в інформаційній сфері. Обґрунтовано доцільність використання правового моделювання в правотворчій та правозастосовчій практиці, що дозволяє уникнути негативного впливу на свідомість дитини. Установлено, що ІБ як складова національної безпеки потребує використання всього комплексу механізмів моніторингу та прогнозування, але має свою специфіку. По-перше, ІБ є одним із найбільш технологічних секторів безпеки, що активно використовує сучасні інформаційні технології. По-друге, ІБ розглядається

мінімум у двох аспектах: технічному (кібербезпека і кібервійни тощо) та ідеологічному (пропаганда тощо). По-третє, дані моніторингу, висновки та рекомендації, що надає ІБ, є основою прогнозування у всій галузі національної безпеки. Розглянуто особливості напрямів прогнозування в сфері інформаційної безпеки в контексті розвитку сучасних інформаційних технологій. Зазначено проблемні питання кібербезпеки та запропоновано шляхи подолання кіберзлочинності.

Statement of the problem

The emergence of an information society in Ukraine and in the world is now accompanied by an update and an aggravation of information confrontation at the regional, national and international levels. The shift of emphasis in the conduct of military conflicts to the integrated use of military and non-military tools (economic, political, information-psychological, etc.) fundamentally changes the character of transformation processes in modern society. Threats to the information security of man, society and the state are becoming more dangerous, and the negative information impact on the individual and social consciousness is becoming more significant. Information threats are of particular concern to the child, as a subject of public relations, who requires special protection and care by the state and society in accordance with the legislation of Ukraine and the rules of international law.

Analysis of recent studies and publications

Question of cybersecurity in Ukraine and other countries was investigated by of V.M. Butuzov [1], V.B. Vehov [2], V.A. Golubev [2], B.P. Smagorinskii [2], O.O. Kirbaitev [3], P.D Bilenchuk [5], B.V. Romanyuk [5], V.S. Zumbalyuk [5], I.D. Gavlovskiy [5], D.A. Niculesko [6].

Objectives of the article

The purpose of the article is to develop recommendations for overcoming cybercrime based on the study of cyber security in Ukraine.

The main material of the research

Modern transformational processes in the information sphere significantly influence the formation of the child's consciousness and perception of the outside world, and the information of negative content can distort the outlook of the child, replace its moral and ethical values, interfere with the formation of a holistic and harmonious personality.

Among the main priorities for information security, in accordance with the provisions of paragraph 4.11 of the National Security Strategy of Ukraine, the following have been recognized: ensuring the offensive of information security policy measures on the basis of asymmetric actions against all forms and manifestations of information aggression; counteraction to information operations against Ukraine, manipulation of public consciousness and dissemination of distorted information, protection of national values and strengthening of the unity of Ukrainian society; development and implementation of coordinated information policy of public authorities.

Analysis of the current state of information security in Ukraine suggests that the system of protection of information security of the child in Ukraine remains insufficiently effective and in need of a radical transformation in accordance with the current challenges and threats in the information sphere. The legal provision of information security of the child develops fragmentarily, situationally, in the absence of a systematic approach and a unified information policy of the state, which reduces the effectiveness of counteracting information challenges and threats and complicates the organization of preventive measures to prevent them.

As an example, the lack of a unified state information policy, including the issues of coverage of the situation in the east of Ukraine, the monopolization of the media, whose editorial policy depends on the preferences of their owners, leaves practically without leverage the influence of central and local executive authorities on prevention of information challenges. Given the increasing level of dangers for the child in the information society, there is a need to use legal modelling in law-making and law-enforcement practice, which will prevent the possibility of negative information influences on its consciousness. Developing a preventive legal model in this area is possible provided that methods of legal modelling of the development of social processes based on the comprehensive analysis and forecasting real and potential threats to information security of the individual, society and the state are used. This requires the creation of an integrated system for assessing information threats, as outlined in the priorities of the National Security Strategy of Ukraine. Topical in this issue is the elaboration and implementation in Ukraine of the Internet Organised Crime Threat Assessment (IOCTA), which has been developed by the Europol.

In accordance with the fundamental provisions of the Doctrine of Information Security of Ukraine, securing information sovereignty, preventing information aggression, expansion and information blockade of Ukraine by foreign states, organizations, groups and persons is a priority task of our country's politics. Information security of the state is an integral part of each area of national security.

At the same time, information security is an important independent area of national security, which characterizes the state of protection of national interests in the information sphere from external and internal threats and is a set of information-psychological (psychophysical) and information-technological security of the state. The relevance of this topic is that information security is an important component of national security. As scientific and technological progress increases, the importance of the information security of the citizen, society, and the state will increase.

That is, information has become a factor that can lead to major technological accidents, military conflicts and defeats in them, disorganize public administration, financial system, work of scientific centres, and the higher

the level of intellectualization and informatization of society, the more necessary is reliable information security, since the realization of people and states are increasingly realized through informatization.

Given the fact that under the influence of information attacks can intentionally change the outlook and morality of both individuals and society as a whole, alien interests, motives, lifestyles, the analysis of the essence and forms of manifestations of modern methods of latent aggressive influence comes to the fore. The manifestation of actions that have a purposeful aggressive nature and which is contrary to the interests of national security, developing mechanisms to counteract them in all directions.

The information security is a state of protection of vital interests of a person, society and the state, in which harm is prevented through: incomplete, untimely and unreliable information used; negative information impact; negative consequences of the use of information technologies; unauthorized distribution, use and violation of the integrity, confidentiality and accessibility of information. The lawmaker and the legislator of Ukraine have a very poor understanding of the essence and mechanisms of law-making.

They also do not completely understand the difference between concepts and categories such as doctrine, concept, strategy, program, tactics, etc. It also seems that the last unknown cause and effect connection between socio-political phenomena and, first of all, the codes, laws, resolutions of the Verkhovna Rada of Ukraine, normative-legal acts of the President and the Cabinet of Ministers of Ukraine, which are clearly defined in the parliamentary-presidential republic and therefore "weight".

Based on the definitions that doctrine is a guiding theoretical or political principle; concept – a system of views on phenomena, a single, defining concept; strategy is a general, non-detailed plan of a specific activity covering a long period; program – a pre-approved (defined) action; tactics – a conceptual action that takes the form of one or more specific tasks, it becomes apparent that: the doctrine must be adopted by a legal act such as the Law of Ukraine for a term up to 20 years), the concept – by a resolution of the Verkhovna Rada for a term of up to 10 years, the strategy – by the Decree of the President of Ukraine, and as evidenced by the world practice – at the time of his election, the program – by the central executive bodies for 1 year with certain tactical methods of its implementation. But as noted above, our ruler creates his own path, known only to him, contrary to common sense.

In the current conditions of development of Ukrainian statehood, the following are initially adopted: the Cabinet of Ministers Resolution, then, Presidential Decrees on Information Security Issues and only then the Law of Ukraine of the global importance for the state "On National Security of Ukraine", which does not provide for amendments to the normative acts of the President and the Cabinet of Ministers Ukraine on information security issues.

We further consider it advisable to briefly comment on them. In recent years, there has been a worsening criminogenic situation in Ukraine. Due to the increased fight against crime, the flow of information processed by law enforcement agencies has increased, the number of urgent documents requiring immediate resolution has increased. The volume of existing databases has grown significantly, reaching the point where the available technical means and technologies do not allow the processing of the incoming information promptly and qualitatively.

It should be noted that every state must protect its independence, territory, interests of its people, citizens, interests of economy and so on. The state owns certain information that cannot be disclosed to the general public. According to Article 20 of the Law of Ukraine "On Information", information on the access order is divided into open and restricted information. Any information is open to the public except for information that is restricted by law.

Restricted information is confidential, confidential and proprietary information. Information security in the bodies of the National Police of Ukraine is to preserve the integrity of the information circulating in the police and has its own peculiarities. First of all, it concerns information containing state secrets. State secret is a type of classified information that covers information in the fields of defence, economy, science and technology, foreign relations, state security and law enforcement, disclosure of which could be detrimental to national security Ukraine and which are recognized as state secrets and subject to state protection. The list of the information containing the state secret, marked in the “Summary of the information constituting the state secret”, was approved by the order of the Security Service of Ukraine from August 12, 2005, No. 440. In addition, the protection requires confidential information in automated systems, telecommunication channels and in working premises units of the National Police of Ukraine. Law enforcement agencies also need protection against misinformation.

Security and protection in the information system should be built taking into account a comprehensive approach to building a security system, which envisages the integration of the necessary measures and information security measures at all levels of the information security system. That information influence on the state, society, citizen is now more effective and economical than political, economic and even military.

Countries with more advanced infrastructure, setting technological standards and providing their customers with resources, determine the conditions for the formation and operation of information structures in other countries, have a significant impact on the development of their information spheres. 12 years later, in a military conflict with the Russian Federation, a legislator in the Cyber Security Strategy of Ukraine approved by the Presidential Decree of March 15, 2016, № 96/2016, it is emphasized that cyberspace is gradually being transformed into a separate, along with the traditional “Earth”, “Air”, “Sea” and “Space”, a sphere of warfare, in which the relevant units of the leading powers of the world are increasingly active. Given the widespread use of modern information technologies in the security and defence sector, the creation of a unified automated control system of the Armed Forces of Ukraine makes our country's defence more vulnerable to cyber threats. In modern conditions,

economic, scientific, technical, information, public administration, defence-industrial and transport complexes, electronic communications infrastructure, security and defence Ukraine is becoming more vulnerable to the intelligence and subversive activity of foreign intelligence services in cyberspace. Increasing intelligence and subversive and terrorist activity in Ukraine, placing on Ukraine's intelligence service and the Ukrainian security service topical tasks of ensuring information security of the state, in particular, and information security in its foreign countries institutions (FCI).

The current stage of the development of scientific and technological progress, the use by the diplomatic services of modern technical means of processing and transfer of information, the latest information technologies have formed a fundamentally new environment for the functioning of the bodies of the diplomatic service abroad, which contains significant risks and threats to their safe activity, and, above all, to effective implementation of their diplomatic mission in secure information conditions. According to experts, the key issues in this area are information security (FCI), creation of safe conditions for working with official and confidential information, prompt exchange of information with the Ministry of Foreign Affairs of Ukraine in order to inform the leadership of the state in a timely and preventive manner and prevent damage to it in political, economic, military-technical, humanitarian and other spheres. features of systemic confrontation, and the infosphere becomes an environment in which it is quite possible to implement threats to the security and stability of countries, forcing changes in approaches to information of organization and operational activities.

The issue of anti-terrorist security and the development of content searches to identify risks and threats of a terrorist nature have been the subject of active scientific research. Mass media can be considered one of the main institutes of modern society, which, by accumulating, analysing and presenting information in a convenient (or beneficial) form, play a huge role in shaping the mass public consciousness, influences the politics and development of public opinion as a whole.

The specific form of modern terrorism is the constitutional war (Latin conscientia – consciousness, conscience) – the war on the defeat of consciousness, the destruction of identity, as well as the human ability to self-identify. The features of the continental war include such features as: latency for a long time; the diversity, flexibility and unpredictability of the means of influence; the use of violent methods of distortion of the information and communication space; erasing a clear demarcation of "friend-enemy"; destruction of spiritual values, perceptions of good and evil, the ability of man to free self-identification and others.

The Security Service of Ukraine is defined by the legislator as a state special purpose body with legal functions that ensures state security, that is, it is one of the subjects of ensuring the national security of Ukraine, and, therefore, one of the leading subjects of the implementation of state policy in the information sphere. According to the Law of Ukraine “On the Security Service of Ukraine”, military counterintelligence bodies are created for the counterintelligence provision of the Armed Forces of Ukraine (AFS) and the State Border Guard Service of Ukraine and other military formations stationed in the territory of Ukraine.

One of the important components of the counterintelligence provision of the Armed Forces of Ukraine is the implementation of measures in the interests of ensuring information security of the Armed Forces. In the Armed Forces of Ukraine there is a system of cybersecurity, the functions of which are the control (monitoring) of cybersecurity; conducting operations (actions) in cyberspace; development of special software; protection of information and telecommunication systems against cyber-attacks; control of information security in information and telecommunication systems; creation of complex information security systems in information and telecommunication systems; antivirus protection in information and telecommunication systems.

The issue of studying the specifics of the formation and use of social media resources is updated, given that in an information society, dominant functions and processes are increasingly organized on the principle of networks. Nowadays, social networks are associated with a special type of communication that is the basis for creating and maintaining personal and professional connections between people.

As G. Bakulev rightly points out, “new media often give people what they want, even if the long-awaited consequences may prove negative. Unlike the usual media, they have no connection with other traditional social institutions that have a social responsibility. Adapting to new media and their specificities often undermines existing social connections. The changing media industry is forcing other social institutions to change, including political, religious, business, military and educational institutions.”

Social networks are increasingly embedded in society, causing socio-cultural shifts in it. At the same time, social processes are also heavily projected onto social media. The structure, content of social networks, topics of communication of users reflect the actual problems of public life. First of all, we are talking about the creative self-realization of the individual, their self-expression through communication, establishing professional and personal relationships, the development of social journalism.

Today's stage of civilization is characterized by the emergence of a global information society, in which information is the main strategic resource. New information and communication technologies are increasingly penetrating practically all spheres of society, changing the working conditions and life of a person, forming new needs, stereotypes of behaviour, as well as new ideas about quality of life, space and time.

In the conditions of dissemination of the latest information technologies, creation of state and non-state registers, information systems and databases, formation of national and global information space and development of information society, the problem of personal data protection becomes one of the key elements in the system

of protection of human rights and security. Law enforcement practices in this area in Ukraine remain rather ambiguous.

The issue of personal data protection is currently of concern to many citizens of Ukraine regarding the possibility of unauthorized distribution and unauthorized use of this data. Despite the existence of a legal mechanism for personal data protection (the Constitution of Ukraine, international standards, the EU Data Protection Package, the Law of Ukraine "On Personal Data Protection"), in real life, its effectiveness is rather doubtful. Objectively, this can be determined by the difficulties of political, legal and socio-economic transformations taking place in Ukraine.

On the other hand, it is widely believed that the problems of personal data protection do not belong to the most urgent in the current conditions. This does not take into account the fact that at present there is no sphere of human activity, society and state where personal data would not be processed. In addition, the provisions of the Law of Ukraine "On Personal Data Protection" are far from perfect. In particular, it is necessary to create an effective mechanism for the protection of the human right to their personal data, to improve the conceptual categorical apparatus, to introduce a mechanism for establishing a personal data subject's privacy regime, improvement of sectoral legislation (health care, education, etc.), which in one way or another regulates the issue of protection of personal data in a specific sphere of human life, etc. According to the study, basic laws on personal data protection in most European countries were adopted in the late XX – early XXI century. Despite the divergence of legal systems, the principles of personal data protection legislation are based on the same principles set out in international standards. The protection of personal data is seen in the political systems of different countries on the European continent as an integral element of democracy and the rule of law. The problem of cybercrime, at the present stage of historical development, acquires a global dimension and becomes a threat to the information society. In the process of formation of the concept of "cybercrime", a number of stages have taken place, and we have received reflections in the normative and legal acts of the national. The fight against cybercrime requires an active and close international co-operation of all modern states. One of these steps is the signature in the leaf 2001 the Council of Europe, and also the United States, Canada, and Japan, the Convention on Cybercrime. The prospect of overcoming the problem of cybercrime may be a further deepening of the cooperation of states and international institutions in the detection, but a major pre-emption, of cybercrime. Considering the counteraction to crimes in the field of computer technology, from the point of view of international cooperation, it is necessary to understand the reasons for their increased danger for the world community and to identify the main problems caused by certain peculiarities inherent only to this type of crime, namely: international nature, that is a criminal has the possibility of getting unauthorized access to any computer system that is connected to the World Wide Web Internet (irrespective of state boundaries and distance to it); a high level of latency, the reasons being: the complexity of the practical detection of crimes by law enforcement agencies; not the will of the victim to report the crime committed against her; erroneous (or deliberate) "write-offs" of the consequences of misconduct on account of hardware and software problems of computer systems; insufficiency of standardized methods of disclosure and investigation of specified crimes, established mechanisms of interstate interaction in investigations; significant level of dependence of the modern society on information technologies, covering almost all spheres of human activity and functioning of the state (banking, energy, transportation, defence and other spheres), and can be considered as potential cyber-attacks.

Conclusions

The information space, the main components of which are information resources, means of information interaction and information infrastructure, is an area of modern social life in which information communications play a leading role.

The objective process is the gradual but steady entry of the national information space into the European and world information sphere, in the context of which a legitimate question arises about its protection, as one of the components of the national security of Ukraine. However, the implementation of this issue in practice is immediately confronted with the need to observe the rights and fundamental freedoms guaranteed by international normative acts and the Constitution of Ukraine, especially in the area of access to information.

The right of access to information is a constitutional right of a person, which is provided for and guaranteed by Art. 34 of the Constitution of Ukraine, namely: the right of everyone to freedom of thought and expression, to express their views and beliefs freely; the right to freely collect, store, use and disseminate information, either verbally, in writing or in any other way of your choice. The exercise of these rights may be restricted only in cases specified by law; however, the provisions of Part 2 of Art. 15 of the Constitution of Ukraine contains an imperative rule that censorship in the state is prohibited.

In our opinion, the resolution of the identified problematic issue requires clarification of the essence of the specified category. Thus, the concept of censorship (Latin censura – "rigorous judgment", "principled criticism") has no universal definition and, for the most part, is perceived solely as a negative socio-cultural phenomenon. At the same time, all developed democratic states have a certain censorship regime. Usually, censorship is understood to mean the system of control over government institutions over the content and distribution of information in the form of printed matter, music and scenic works, works of fine arts, film, photo materials, radio and television broadcasts, web-based resources and, in some cases, private correspondence, to limit or prevent the dissemination of ideas and information deemed harmful, undesirable to the state or society as a whole critical infrastructure facilities. The constituents of such a system must prevent the possibility of committing sabotage and subversive actions or minimize their consequences in political, economic, military, and cyberspace.

A characteristic feature of the “hybrid” war is that the enemy will seek to defeat not only the units of the regular army, but also the objects of critical infrastructure that are deep in the territory. In order to implement such a scenario, combat capabilities and ways of using diversionary intelligence groups are constantly being improved. The continuous development of forms and methods of sabotage in the rear of the enemy, improving the tactical and technical characteristics of high-precision weapons and conventional weapons of destruction, threats in cyberspace require very high requirements for a national system of anti-sabotage protection of critical infrastructure.

References

1. Butuzov, V. M. (2010). Pro spivvidnoshennya ponyat′ «komp'yuterna zlochynnist» ta «kiberzlochynnist» [Of Correlation of of concepts of «computer criminality» and «cyberbuck criminality»]. Informatsiyna bezpeka lyudyny, suspil′stva, derzhavy - Informative safety of man, society, state, 1 (3), 18.
2. Vehov, V. B., Golubev, V. A. (2004). Rozsliduvannya komp'yuternykh zlochyniv u krayinakh SND [Investigation of computer crimes in countries the of CIS]. Volgograd: MVD
3. Kirbaitev, O. O. (2010). Komp'yuterni zlochyny: realiyi suchasnosti, problema borot′by z nymy ta dostovirni sposoby yikh vyrishennya [The Computer crimes: realities of contemporaneity, problem of fight against them and credible ways of their decision]. Retrieved from http://web.znu.edu.ua/ herald/issues/2010/Ur - 1-2010/165-170.pdf
4. Sait Upravlinnya finansovykh rozsliduvan′, Uryadova sluzhba finansovoho monitorynhu Ukrayiny [Site of the Department of financial investigations, Government of service of the financial monitoring of Ukraine]. Retrieved from http://sfs.gov.ua/
5. Bilenchuk, P. D., Romanyuk, B. V., Zumbalyuk, V. S. (2002). Komp'yuterna zlochynnist [Computer criminality]. Kyiv: Atika
6. Niculesk,o D. Kiberbezpeka: vrazlyvi momenty [Cybersecurity: vulnerable]. Retrieved from http://yur-gazeta.com/publications/practice /inshe/kiberbezpeka-vrazlivi-momenti.html
7. Activity of government of Czech Republic is in towards integration to NATO. Retrieved from http://osvita.ua/vnz/reports/world history/ 4787.
8. Site of informative security of Czech Republic Service: Division of «Pronas». Retrieved from https://www.bis.cz/o-nas.
9. Site of informative security of Czech Republic Service: Division «As work». Retrieved from https://www.bis.cz/jak-pracujeme.
10. Site of informative security of Czech Republic Service: the Annual report for 2017. Retrieved from https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/ 2017-vz-cz.pdf.