JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 December Volume 10 Number 2
http://doi.org/10.9770/jssi.2020.10.2(9)

Scopus®

LEGAL ASPECTS OF INFORMATION SECURITY MANAGEMENT IN THE CONDITIONS OF UKRAINE'S EUROPEAN INTEGRATION

Vladislav Fedorenko[1], Nataliia Lytvyn[2], Dmytro Luchenko[3], Iryna Panova[4], Nelli Tsybulnyk[5]

[1]Ministry of Justice of Ukraine, Honored Lawyer of Ukraine, 26, L. Ukrainka Boulevar, office 501, Kyiv, 01133, Ukraine
[2]State Fiscal Service University of Ukraine, 08201, Kyiv region, Irpin, str. University, 31, Ukraine*
[3]Yaroslav Mudryi National Law University, 61024, 77 Pushkinskaya Street, Kharkiv, Ukraine
[4,5]Kharkiv National University of Internal Affairs, Kharkiv, Lev Landau Avenue, 27, Kharkiv, 61000, Ukraine

E-mail: [2]natlyt@ukr.net (Corresponding author)*

Received 15 March 2020; accepted 28 October 2020; published 30 December 2020

Abstract. It has been revealed that the legal and doctrinal basis of information security in Ukraine developed symptomatically and haphazardly. This is largely due to the fact that modern research methods are based on different worldview positions, solve research problems in different ways, and also use excellent research strategies. In addition, information security was primarily viewed as the information security of the state. Subsequently, the intensification of informatization processes in all areas, especially the growth in the importance of technical protection of information, led to the formation of legal support for the protection of information as an integral component of the security of enterprises, institutions and organizations, as well as individual sectors of the economy. At the turn of the millennium, the question of international information security, as well as cybersecurity as part of information security, became acute. The stages of the formation of Ukrainian legislation in the information sphere in general, and information security in particular, have been analyzed, and it has been found that at each of these stages, the information security of a person remained a secondary issue. Increasing the efficiency of administrative and legal support for information security in Ukraine is possible through the implementation of a set of legal measures, which include: clear reflection in law and state institutions of the orientation on the combination of public and private economic interests in the information sphere; constant and consistent use of all human rights mechanisms and procedures to overcome conflicts in the information sphere; raising the legal level of consciousness and activities of civil servants, representatives of all branches and levels of government, and the country's population.

Keywords: information security; administrative and legal support; cyber security; information technology; human rights mechanism.

Reference to this paper should be made as follows: Fedorenko, V., Lytvyn, N., Luchenko, D., Panova, I., Tsybulnyk, N. 2020. Legal aspects of information security management in the conditions of Ukraine's European integration. *Journal of Security and Sustainability* Issues 10(2): 103-115. http://doi.org/10.9770/jssi.2020.10.2(9)

JEL Classifications: F35; F42

1. Introduction

The analysis of social processes taking place in recent years under the onslaught of information expansion in all spheres of life in Ukraine and the world allows to talk about the approach to the global information society. At the same time, opportunities for the onset of desired and threatening consequences both for society as a whole and for the individual are created. A modern person in a society that goes to the information things, immersed in the world of technology and unnecessary information. Information technology (IT) is actively used in every sphere of society's life, which leads to an increase in informational influences.

The dynamic development of reality also requires a revision of approaches to understanding the security of society, the state and, above all, a person. The vision of security that emerged at the end of the 20th century,

which was based on the absence of danger or neutralization of threats, and was, first of all, adapted to the needs of the state, is not able to reflect the essence of human security in the modern globalized and information-rich world.

At the end of the XX century, information and legal research focused on the study of the characteristics of social relations that arose in connection with the increasingly active use of IT and an attempt to settle the modified relations. At the same time, two tendencies of legal regulation of relations in the information sphere have developed in the world: to use by analogy the legislation, which exists, while creating new norms only on the basis of realities that rise up in connection with comprehensive informatization; or to create new legislation.

At the same time, the regulation of existing information relations was insufficient, which emphasized the need for effective implementation of the predictive function of law. The formation of legislation does not keep pace with the achievements of scientific and technological progress, in connection with which new social relations arise, which, quite often, require, first of all, ethical and only then legal assessment by society. At the same time, an ordinary citizen finds himself in the same situation as politicians - a significant level of entropy with an excess of information and the requirement to make decisions quickly. Thus, next to external (objective) threats to information security of a person, which are associated with the illegal use of IT, insufficient or ineffective legal regulation of information relations, internal (subjective) ones rise - the lack of an appropriate level of information culture (including literacy, unwillingness to resist negative or excessive informational influences, inability to adapt to new social conditions associated with a constant increase in information saturation in all spheres of life).

Studies of the realities of society, which strives for information one and conditions for the safe existence of a person in it, indicate the need to identify patterns and trends in the emergence and actualization of information threats, as well as to determine the boundaries of the necessary and possible state intervention through legal support and institutional protection. In addition, it is necessary to study the role of a person in ensuring its own information security in the context of globalization, the development of a democratic rule of law, and the formation of civil society. Therefore, the legal foundations of human information security should be studied not detached from the information security system of society, the state and the global information security of mankind but taking into account their mutual determination and constant interaction.

2. Literature Survey

The development of security science in the direction of information security significantly depends on the immersion of a particular society and state in the reality of an information explosion and the formation of an information society (Zhang, D. (2018)).

The level of development and use of IKT in the world is very uneven, in particular, information problems of 60% of the population are at a completely different level (Shafqat, N., & Masood, A. (2016)). However, this does not mean that they do not exist.

A person is always “doomed” to search, evaluate, and protect information (the difference is only in its content - information about hunting places, a source of water, another tribe or trade secrets and personal data), that is, information activity, which is inextricably linked with information security (Ahmadi, R., & Movahed, SAHS (2019)) Only if the information society is formed, the importance of the latter is steadily growing.

The overwhelming majority of scientific works on the topic of information security begin with justifying its relevance (Kharytonov, E., et.al. (2019)), increasing the penetration of information technologies into all spheres of society (Vance, A., Siponen, MT, & Straub, DW (2020)), as well as the formation of the information society as a new stage in the development (type) of society (Spanos, G., & Angelis, L. (2016)), in which the issue of information security acquires new significance and is the subject of legal regulation, one of the main areas of national security and state security, as well as a prerequisite for respect for human and civil rights and freedoms. Thus, the phenomenon of information security is viewed through the prism of a person’s practical-activity re-

lationship to the state and society, based on the needs and interests of security objects and subjects (Parvin, S., Sadoughi, F., Karimi, A., Mohammadi, M., & Aminpour, F. (2019); Stefaniuk, T. (2020)). Undoubtedly, conscious security can have a decisive influence on the content and development of social processes (da Veiga, A., Astakhova, L.V., Botha, A., & Herselman, M. (2020)). This explains the relevance of the study of information security as a scientific category and as a social phenomenon (Haqaf, H., & Koyuncu, M. (2018)).

Information confrontation, like any other, is a naturally conditioned element of competition in the modern globalizing world. Therefore, the problem of information and cyber security acquires particular importance in order to establish a balance of interests of the individual, society, state, and international community (Schatz, D., Bashroush, R., & Wall, J. (2017); Tvaronavičienė, M., Plėta, T., Della Casa, S., Latvys, J. **(**2020)).

Information security as a scientific category is interpreted in various ways (Mandritsa, I. V., Stefano, S., Mandritsa, O. V., & Petrenko, V. I. (2016); Ključnikov, A., Mura, L., Sklenár, D. (2019)). There are both doctrinal, encyclopedic, and legal definitions (Kerr, J. A. (2018)). At the same time, methodological approaches, logical ways of their formation and consolidation, and the scope of existence and applied use differ significantly. This is also due to the fact that the category of safety is ambiguous and is determined depending on the scientific field in which it is studied.

3. Methods

The methodological basis of the research was a set of methods, approaches, and techniques of scientific knowledge – both general scientific and special: dialectical, historical and legal, logical, system analysis, statistical, systemic and structural, comparative and legal, logical and semantic, formal legal, etc... To use the modern achievements of world science, a transdisciplinary approach was chosen as one of the main ones, as one of the main ways to study complex multifactorial problems of the 21st century. The leading of the classical methods was the general scientific dialectical method of cognition, which made it possible to study the socio-legal nature of human information security in connection with the modern socio-political situation, change in the historical type of society and socio-economic formation, as well as the formation of the global information society.

The philosophical arsenal of legal hermeneutics, ontology, and axiology is also used in the work. In particular, the historical and legal method was used to clarify the features of the formation and development of legal support for information security, as well as to study the prerequisites for the formation of information human rights as the ontological essence of its information security. The system-structural method made it possible to consider the internal structure of information security, to determine the place and correlation of human information security with information security as a complex social and legal phenomenon, and to outline its place in the national security system, and also and to promote the definition of research methodology for the system of legal support of information security. The statistical method made it possible to identify trends in the formation and actualization of threats to human information security. The classification method was used to comprehend the multitude of threats to human information security, to identify social groups that have certain specific characteristics that determine the generality of approaches to their insurance in the information space. The comparative method was used to compare the legislative regulation of relations in the information sphere of different countries of the world, as well as in the study of acts of international law, and to determine the prospects for adapting national legislation to international standards in the studied area. With the help of the formal legal method, the norms of constitutional, administrative, information law, and other branches of law and legislation, which determine the legal foundations of human information security, were studied. As well, this method was used to formulate the author's definitions of concepts. The methods of theoretical and legal forecasting and modeling were used to put forward and substantiate proposals for amendments and additions to the current legislation on human information security.

The regulatory framework of the study is the national legislation of Ukraine and foreign countries (EU countries, the USA, the EU Eastern Partnership countries, the Russian Federation, and the PRC), as well as international legal acts.

The scientific and theoretical basis of the study is theoretical and methodological developments and monographic studies of specialists in the general theory of state and law, in the fields of constitutional, administrative, information, international law and scientific developments in security theory, sociology, psychology, and political science.

The empirical basis of the study was the materials of the rule-making practice of public authorities, political and legal journalism, reference books, statistical materials, case law of Ukrainian and foreign courts, as well as the European Court of Human Rights on the topic of the study.

4. Results

At the beginning of the XXI century, the activity of the state in the legal field has changed significantly and dynamically. However, the changes that have occurred so far have not received their systematic, comprehensive scientific and theoretical analysis in the field of information security. This especially concerns the issues of guarantees and protection of the rights and freedoms of citizens, maintaining the information security of the individual, which is becoming an independent subject of state policy.

It is not by chance that the current development of a person and society is characterized by the development of a legal lifestyle as one of the most optimal value institutions for survival and achieving well-being. It is obvious that ensuring information security at the present stage is simply impossible without the active influence of law as a system of norms and the legal system of society. In the complex interweaving of the sphere of security and law, as a normative regulator, a new form of information security is born, which provides public life with predictability, stability, adequacy, and certainty. It is information security as a state of protection of the interests of the individual, the rights and freedoms of man, society and the state that makes it possible to see and evaluate the normal functioning of the political and economic system of the state. The information security mechanism provides the information sphere with additional guarantees of viability and normal functioning.

As a regulated system, the information security mechanism itself requires regulatory impact. The interaction of the constituent links (elements) of the information security mechanism is embodied in legal relations, in a special subject-object environment, in corresponding relationships, and the implementation is carried out in acts of a volitional nature, which are applied taking into account the place and role of one or another link in the information security system.

The theory of information society development shows a relatively low degree of criticality of research in regard to the opportunities that open up through the use of information technology. This leads to insufficient attention to new types of dangers, threats that arise in society as a result of the negative effects of information technology. The problem of information security arose on the basis of a global contradiction between the capabilities of information technologies, on the one hand, and the negative effects, dangers, and threats of their use for destructive purposes in relation to the individual, society, and state, on the other hand.

Currently, in the context of the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their member states, on the other hand, one of the main strategic priorities is the development of the information society and the introduction of the latest information and communication technologies in all spheres of public life and in the activities of public authorities (On the ratification of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (2014)).

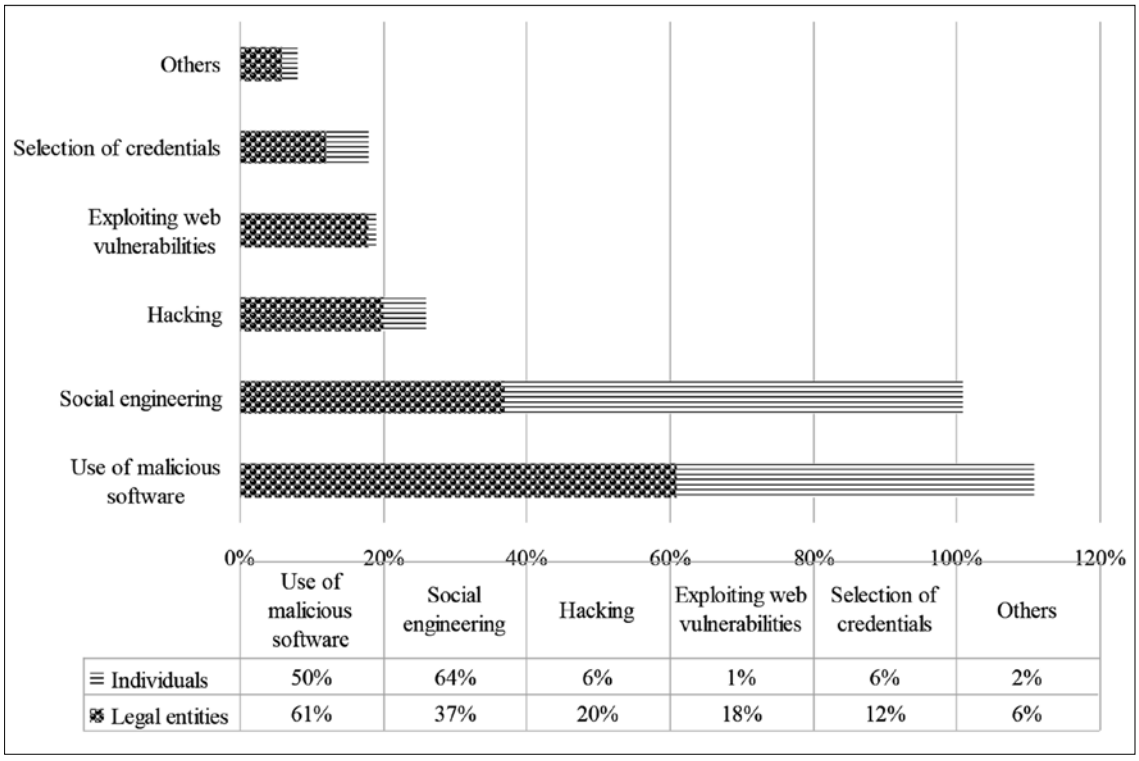
As indicated in the "Strategy for the Development of the Information Society in Ukraine" (adopted on May 15, 2013), the goal of the formation and development of the information society in Ukraine is to improve the quality of life of citizens, to ensure the competitiveness of Ukraine, to develop the economic, socio-political, cultural, and spiritual spheres of life society, to improve the public administration system based on the use of

information and telecommunication technologies (On approval of the Information Society Development Strategy in Ukraine (2013)).

The statistical data on the relevance of cyber threats in Ukraine for 2019 have been considered. The rapid informatization of society has a positive effect on many areas of the economy: the financial industry, trade, industry, health care, education, science. Today information technology is an integral part of not only successful business but also state policy. However, criminals learned to use them for their own purposes, which gave rise to a confrontation with information security specialists. This struggle contributes to the continuous improvement of the methods and tools used by the attacker, which inevitably generates an increase in the number of cyber threats.

The cyber threat is a combination of factors and conditions that create a threat of information security breach. In this study, the authors consider cyber threats from the point of view of the actions of cybercriminals in cyberspace aimed at penetrating an information system with the aim of stealing data, money, or with other intentions that potentially lead to negative consequences for the state, business, or individuals. The actions of criminals can be directed to the company's IT infrastructure, work computers, mobile devices, other technical means, and, finally, a person as an element of cyberspace.

Figure 1 shows the methods of attacks on legal entities and individuals in Ukraine in 2019.



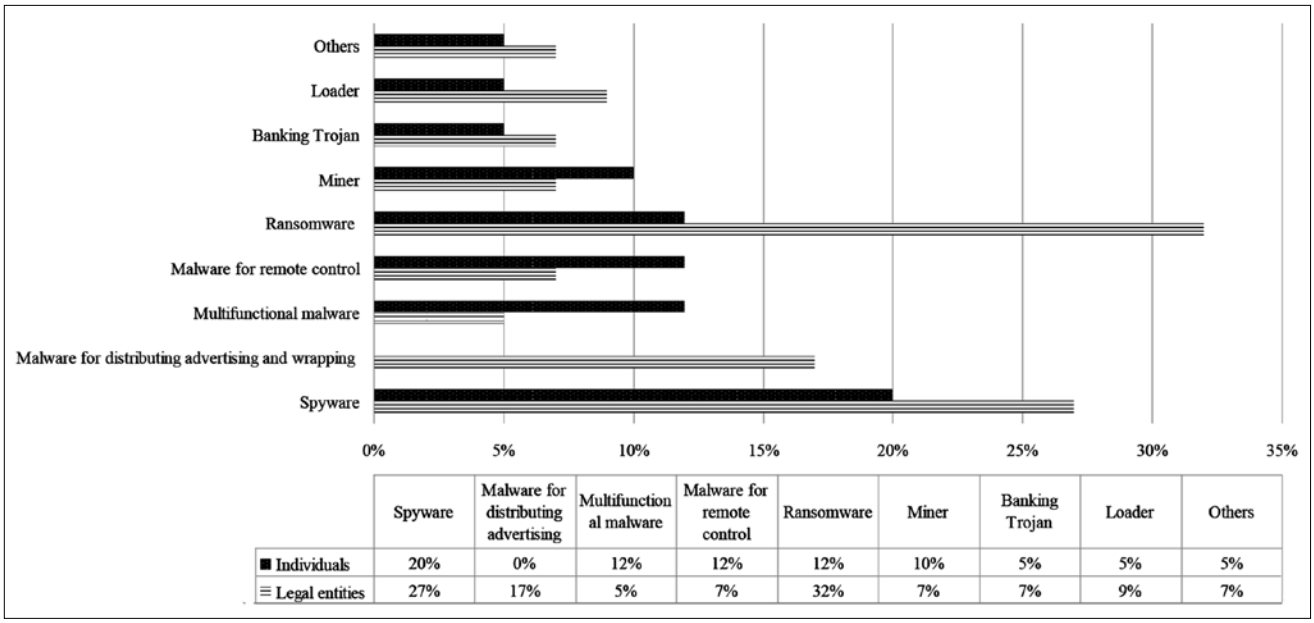
	Use of malicious software	Social engineering	Hacking	Exploiting web vulnerabilities	Selection of credentials	Others
Individuals	50%	64%	6%	1%	6%	2%
Legal entities	61%	37%	20%	18%	12%	6%

Figure 1. Methods of attacks in Ukraine (2019)

Source: compiled on the basis of https://cert.gov.ua/

Let's take a closer look at each method and point out which objects and industries suffered most from these categories of attacks.

The use of malware - Figure 2.



	Spyware	Malware for distributing advertising	Multifunctional malware	Malware for remote control	Ransomware	Miner	Banking Trojan	Loader	Others
■ Individuals	20%	0%	12%	12%	12%	10%	5%	5%	5%
≡ Legal entities	27%	17%	5%	7%	32%	7%	7%	9%	7%

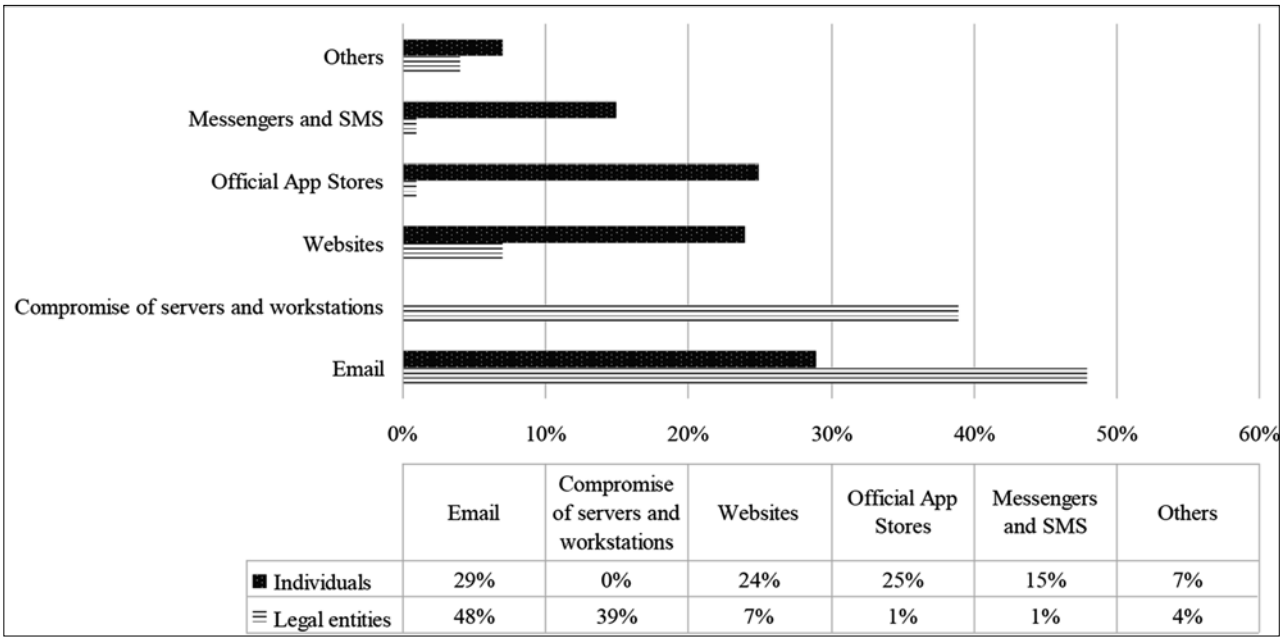
Figure 2. Types of malware in Ukraine (2019)

Source: compiled on the basis https://cert.gov.ua/

The share of multifunctional Trojans continues to grow. For example, the modular DanaBot Trojan, about which it was written in the first quarter, is now capable of acting as a ransomware. On the contrary, the activity of one of the most widespread ransomware GandCrab began to decline, and its operators announced the end of the malicious campaign. A few weeks after the news of the cessation of the development of the ransomware Trojan, it became known that cybersecurity specialists gained access to the GandCrab servers, and with it the encryption keys, thanks to which a decryption program was created for the latest version of GandCrab, which allows to recover files encrypted by it.

Despite these events, the share of ransomware attacks remains high. This is because you do not need to develop a unique code to create a simple ransomware. Most of the new copies of ransomware are very similar to their predecessors since cybercriminals often do not develop the ransomware from scratch but purchase ready-made code or a subscription (ransomware as a service) on the dark web. Thus, with a minimal start-up capital, ransomware can bring owners a good income.

Since April 2019, there have been periodic reports of attacks by the new ransomware Sodinokibi. At least three IT service providers have already become victims. Cybercriminals used remote administration tools (Webroot and Kaseya) to infect companies with ransomware - clients of compromised IT service providers with the ransomware. However, supply chain attacks are not the only vector for Sodinokibi's spread. The Trojan also spreads through vulnerabilities in Oracle WebLogic Server and phishing emails.
Email remains the most popular delivery method for malware (Figure 3).



	Email	Compromise of servers and workstations	Websites	Official App Stores	Messengers and SMS	Others
Individuals	29%	0%	24%	25%	15%	7%
Legal entities	48%	39%	7%	1%	1%	4%

Figure 3. Ways of distributing malware in Ukraine (2019)

Source: compiled on the basis https://cert.gov.ua/

In the second quarter, experts noted an increase in the spread of Trojans through ISO files (digital images of CDs). For example, AgentTesla, LokiBot, NanoCore are distributed this way. ISO images are often not detected by antivirus solutions because they can be whitelisted. One can suspect something was wrong by the size of the file - a malicious attachment is no more than 2 MB in size, while a legitimate ISO image is usually much larger.

The bitcoin rate is steadily growing and cybercriminals continue to develop software for hidden mining. For example, Sucuri specialists discovered a sample of the miner with improved mechanisms for fixing it in the infrastructure: a special cron script (a script for performing certain actions on a schedule) allows to restore the mining process even if the main malware module was detected and removed from the infected system.

In the second quarter of 2019, cybercriminals actively distributed the AZORult info-stealer. For example, in April, experts of the Positive Technologies Expert Security Center (PT ESC) noted that the RTM group began to use AZORult instead of Pony. In addition, the AZORult Trojan spreads through websites under the guise of various utilities (for example, under the guise of a utility for cleaning and optimizing the work of the G-Cleaner OS or the Pirate Chick VPN client).

In the third quarter of 2019, cybercriminals actively used the set of Azure App Service for various types of social engineering fraud. For example, Azure service is used to quickly deploy phishing pages with bogus authentication forms and to create bogus Microsoft support pages with pop-up messages that a website visitor's computer is allegedly infected with a virus. In addition, cybercriminals send emails offering to download a file by logging in through a fake form previously hosted on the Azure Blob Storage platform. The scale and success of this kind of fraudulent operations are facilitated by the windows.net domain in the address bar and a valid Microsoft SSL certificate. However, the credentials theft scheme is not new, and there are special instructions for users to help set up the automatic blocking of such phishing emails.

As already noted, the rapid rise in the bitcoin rate in the second quarter led to an increase in interest in cryptocurrency, which is what some cybercriminals are trying to make money on. For example, the scammers once again turned to the old scheme, when, allegedly on behalf of famous people or organizations, cash prizes are distributed with the only condition: to receive a reward, it is necessary to make a preliminary transfer of

a small amount of money under the pretext of verifying the address of the recipient of the award. This time, «prizes» in cryptocurrency were handed out allegedly on behalf of John McAfee and Elon Musk.

The YouTube platform is very popular among Internet users, which makes video channels an attractive platform for placing malicious links. During one of these fraudulent campaigns, viewers were offered to watch videos, allegedly teaching how to work with a free bitcoin generator, a link to which was placed in the description under the video. In fact, clicking on the link initiated the download of the Qulab info-stealer. As a result of another similar campaign, malware for remote control of njRAT was distributed via YouTube.

Decentralization and insufficiently clear hierarchy in the activities of subjects of information security in Ukraine, such as the Cabinet of Ministers of Ukraine, the Ministry of Information Policy of Ukraine, the Ministry of Justice of Ukraine, MBC of Ukraine, the lack of unified regulatory foundations for ensuring information security except for the Doctrine of Information Security and the Rules for ensuring the protection of information in information, telecommunication, and information-telecommunication systems approved by the Resolution of the Cabinet of Ministers of Ukraine on March 29, 2006 under No. 373, and detailed legislative regulation of the relevant administrative procedures contribute to abuse in the application of measures of administrative coercion.

The problem of objective selection of means and tools for the investigated sphere of regulation, proper stimulation of actors operating in this area, ensuring the operation of mechanisms due to the nature of the sphere of information security should be solved by the relevant regulatory body on the basis of the current administrative and legal principles.

The specifics of the factual and formal legal grounds and the rules for the appointment of administrative punishment, the administrative process procedure for application, the principles of legality, publicity, individualization, completeness and objectivity of the study of the circumstances of the case, the presumption of innocence, humanity, justice, equality of citizens before the law, and respect for the dignity of the individual should be taken into account by the administrative jurisdiction bodies when applying measures of administrative coercion in the field of information security. These principles are important and are reflected in the current judicial practice.

However, one should take into account the public nature of the state's goal in relation to ensuring information security, which arises from the peremptory norms of the established legal regimes, and the balance and equilibrium of the public and private sides of information legal relations do not always correlate with the tasks of the state in achieving this goal. A number of legal institutions created to maintain this balance, for example, the Institute of the Ukrainian Parliament's Commissioner for Human Rights, are more likely to combat identified abuses of state power than to optimize public administration in the field of information security.

Various spheres of public life dictate the imperative of the differentiated approach to legal regulation. The sphere of security is connected with restrictive and prohibitive norms of law, which are mandatory. Freedom of information relations can be limited by the state in order to ensure information security. Coercive measures, that do not stimulate and do not encourage, are created for the implementation of state goals and are designed to satisfy the state interest. Threats to information security are facilitated by the underdevelopment of the social information infrastructure and the unresolved problems of the state legal system for ensuring law and order, and the underestimation by the executive authorities of the possibilities of administrative coercion in the information sphere. Ensuring law and order is based on measures of administrative coercion, the corresponding legal gaps may result from the inconsistency of these measures with the goal of ensuring the information security of the state.

It is advisable to take into account the ambiguity of the tasks of ensuring information security: both general prevention and stimulation and support of subjects of information activity - owners of critical information infrastructure facilities. The solution of these tasks will contribute to an increase in the efficiency of the subjects

of the investigated activity in countering information security threats.

First of all, the following shortcomings should be eliminated: lack of legislative systematization of administrative-compulsory measures in the field of information security; lack of control over the timeliness and compliance of their application (expressed in the absence of an appropriate authorized control and supervisory body of the executive power conducting the relevant activities); the absence of the executive authority with functions of a predictive and advisory nature in the field of information security, which summarizes law enforcement activities on all enforcement measures and gives recommendations for optimization and unification (possibly a collegial advisory body).

A systematic organization of legislative support for information security is also necessary since a clear regulation of norms is imperative in nature, the rule of law in any sphere of public relations has always been determined. It is necessary to move from a long-term strategy in the field of information security (the Doctrine of Information Security of Ukraine) to the draft Law «On the Basics of Information Security», the adoption of which will serve as the basis for improving the corresponding administrative and compulsory measures.

The effectiveness of organizing and ensuring information security by the National Police is determined by compliance with an objective social purpose, which is expressed in the appropriate conditions and indicators, and all the rest, relatively independent cost-economic, technological, and technical efficiency criteria should be considered as subordinate to social goals, outside of which their application loses meaning and may even hinder the achievement of such goals.

The main criteria for assessing the organization of the activities of the National Police in the field of information security should include: balance of organizational, structural, and functional parameters; adequacy (quantitatively and qualitatively) of resource provision; professional training and readiness of the personnel corps; content filling of management functions, corresponding to the needs of organizational and law enforcement practice; the quality of organizational and law enforcement activities that meets the needs of society and meets the priorities of protecting the rights, freedoms, and life of people.

The assessment should cover the process of performing one of the main tasks of the analytical function of the management activities of the National Police in the field of information security, including a description of the object of assessment, identification of deviations and failures in its functioning, explanation of the reasons and conditions that give rise to them, justification of management decisions and activities.

The analytical function of this task can be ensured in the unity of two directions: increasing the level of methodological and information support of this problem, expanding the range of modern scientific methods and information technologies, which are used in its solution, raising the professional level of personnel employed in this information and analytical field.

5. Discussion

At the present stage of development of the European information space, the main direction of information security is formed within the framework of comprehensive crime prevention programs. Being an objectively necessary function of the National Police bodies, prevention in the field of information security has not been widely used in their activities for a long time. The explanation for the slow development of prevention in the system of National Police bodies, in our opinion, is due to the following reasons: lack of sufficient grounds for the implementation of prevention in the context of socio-political, legal, and economic reforms; the prevalence of opinion about the automatic solution of information security problems as technologies change; advantage in ensuring information security of coercion methods; legal lack of regulation of preventive activities; the negative attitude of the police towards prevention, underestimation of its capabilities and effectiveness in comparison with traditional types of activities - administrative and criminal jurisdictional; lack of internal organizational and personnel prerequisites.

The modern practice of crime prevention in the field of information security does not correspond to the global approaches of its organization in a number of fundamental positions. In Ukraine, the prevention of offenses, within the limits of their competence, is mainly carried out by law enforcement agencies. There is no relevant branch of legislation, which regulates special relations in the field of crime prevention for state and local authorities, non-governmental organizations, business structures, and civil society institutions. There are only individual elements of the state system for the prevention of offenses with insignificant participation of public associations and the population.

In our opinion, taking into account the dynamic development of the national information space, the legal regulation of information security should consist of two levels and include:

- a comprehensive legal regulation of information security management processes, which is enshrined in legislative acts prepared on the basis of a comprehensive scientific examination and substantiation of the stages, methodology, and system of relations that develop in the process of administrative and legal regulation of the activities of security entities in a particular area;

- regulatory and legal regulation of the activities of the National Police in certain areas of information security, which consists of sectoral regulatory legal acts of the National Police, documents of other bodies (for example, the Ministry of Information Policy of Ukraine, the State Service for Special Communications and Information Protection of Ukraine (On the establishment of an interdepartmental working group of the Administration of the State Service for Special Communications and Information Protection of Ukraine and the Ministry of Internal Affairs of Ukraine: Joint Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine, Ministry of Internal Affairs of Ukraine (2015))), which ensure the implementation of state functions in the field of information security.

The relationship between legislative and departmental regulation should be divided according to the characteristics of the management object and the administrative and legal regulation subject, which will answer the question of what legal relations outside the administrative boundaries are formalized (or should be formalized) using regulatory prescriptions. The starting point here is the theoretical understanding of the regulation subject as of social relations that constitute the administrative influence object, which is carried out with the help of legal norms embodied in legislation. They are addressed to the participants in managerial relations, determine the boundaries of possible and proper behavior, thereby influencing the will and consciousness of the relevant subjects.

It is advisable to carry out a comprehensive legal regulation of information security management processes by systematizing and unifying administrative legislation in the field of information security with the help of a codified normative legal act that will establish the initial principles of administrative and public information security in Ukraine.

As such a regulatory legal act, one can propose a joint order of the Ministry of Information Policy of Ukraine, Ministry of Internal Affairs of Ukraine, State Service for Special Communications and Information Protection of Ukraine “On the basics of administrative and legal support of information security in Ukraine”, in which it is advisable to solve the following tasks:

the creation of the same conceptual and categorical apparatus, which very clearly reveals the essence, structure, and content of information security in the field of administrative and legal regulation in Ukraine in accordance with the categories developed by legal science;
the creation of a unified system of specialized executive bodies and executive and administrative bodies of local self-government in Ukraine, which are empowered to ensure the fulfillment of obligatory conditions and information security requirements related to the direct intervention of these bodies in the administrative, economic, organizational, and administrative and other activities of physical and legal persons;
systematization and unification of administrative and legal methods of activity of executive authorities and executive and administrative bodies of local self-government will ensure the fulfillment of obligatory conditions and requirements of information security with direct intervention in the administrative, economic, organizational and administrative, and other activities of individuals and legal entities;

the formal definition of the functions of administrative and legal support of information security, which is transferred to local authorities by state authorities of Ukraine as outsourcing;

the creation of the optimal systemic model of interaction by the method of systematic and sequential change of individual system quality indicators on the basis of reducing the possibility of direct interference in the sphere of technological and civil legal relations, which leads to corresponding changes in the circle and nature of social relations protected by administrative law.

Conclusions

The development of the system for the prevention of offenses in the field of information security that meets modern information security requirements should, in our opinion:
be based on the experience accumulated in the European Union in the development and implementation of national comprehensive programs for the prevention of offenses and legal education of the population;

be carried out within the framework of the unified methodological approach to researching information security problems, taking into account criminology and delictology on the basis of analytical jurisprudence;

rely on a well-thought-out social policy with an optimal combination of purposeful efforts of the state with the initiatives of various institutions of civil society.

The desire to join the European Union creates real preconditions for the formation of the system of government measures to influence the state and dynamics of preventive processes in the field of information security. The practice of organizing preventive activities in the countries of the European Union is based on the principles:

crime prevention is an important component of national public policy;

consistency and an integrated approach to the organization of preventive activities, which provides for the use of all methods of influencing the state of information security. The effective social system of influencing crime reduces people's desire to commit a crime and the ability to implement criminal plans, ensures the cessation of criminal activity, and should be based on the principles of:

synergetic approach to the organization of the mechanism of educational influence of all subjects of preventive activity in the field of prevention of deviant human behavior taking into account victimological prevention, and active involvement of citizens in work on increase of vigilance in the field of information and psychological safety;

adequate material, ideological, personnel, information, and scientific support of this activity;

constant changes in the system of influence on the organization of information security in the context of changes in social and criminal reality.

The study of European experience in the organization of crime prevention in the field of information security allows to identify general trends in the development of prevention systems: the priority of prevention in the policy of counteraction to offenses, ie creating conditions for people not to enter a criminal path but if a person entered or left it (voluntarily or under coercion), then did not end up there again; development and adoption of laws, state and local programs; organization of a single coordinating body; participation in international cooperation in this area through a system of civil society institutions; active regional policy of crime prevention; wide use in the process of organizing preventive activities, which are implemented in various forms at all levels of social management; program-target planning, which is an important tool for the implementation of public policy and allows to organize a clear, well-founded work to achieve goals and objectives.

The adoption of the law "On the principles of the state system of crime prevention" may be an important legal basis for crime prevention, including in the field of information security, taking into account the provisions laid down in regulations that have the same technological system of information security and are common to EU countries principles of crime prevention.

References

Ahmadi, R., & Movahed, S. A. H. S. (2019). Study of artificial neural networks in information security risk assessment. Journal of Management and Accounting Studies, 7(02), 1-10. Available at: http://journals.researchub.org/index.php/JMAS/article/view/597

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713. Available at: https://www.sciencedirect.com/science/article/pii/S0167404820300018

General recommendations for reducing the effects of malware. Available at: https://cert.gov.ua/

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. International Journal of Information Management, 43, 165-172. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0268401218302251

Kerr, J. A. (2018). Information, Security, and Authoritarian Stability: Internet Policy Diffusion and Coordination in the Former Soviet Region. International Journal of Communication (19328036), 12.

Kharytonov, E., Kharytonova, O., Tolmachevska, Y., Fasii, B., & Tkalych, M. (2019). Information Security and Means of Its Legal Support. Amazonia Investiga, 8(19), 255-265. Available at: https://amazoniainvestiga.info/index.php/amazonia/article/view/227

Ključnikov, A., Mura, L., Sklenár, D. (2019). Information security management in SMEs: factors of success, Entrepreneurship and Sustainability Issues, 6(4), 2081-2094. http://doi.org/10.9770/jesi.2019.6.4(37)

Mandritsa, I. V., Stefano, S., Mandritsa, O. V., & Petrenko, V. I. (2016). Mechanism of economic security relativelly to market agents on possible leaks of business information. Modern economy success, (1), 19-31.

On approval of the Information Society Development Strategy in Ukraine (2013). Available at: https://zakon.rada.gov.ua/laws/show/386-2013-p?lang=en#Text

On establishment of an interdepartmental working group of the Administration of the State Service for Special Communications and Information Protection of Ukraine and the Ministry of Internal Affairs of Ukraine: Joint Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine, Ministry of Internal Affairs of Ukraine (2015). Available at: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=E26EA615EF01E8A00DDF183B87CE5FE9.app2?art_id=148413&cat_id=121207

On the ratification of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part (2014). Available at: https://zakon.rada.gov.ua/laws/show/1678-18#Text

Parvin, S., Sadoughi, F., Karimi, A., Mohammadi, M., & Aminpour, F. (2019). Information security from a scientometric perspective. Webology, 16(1), 196-209. Available at: http://eprints.rclis.org/39043/

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. Journal of Digital Forensics, Security and Law, 12(2), 53-74.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. International Journal of Computer Science and Information Security, 14(1), 129.

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. Computers & Security, 58, 216-229. Available at: https://www.sciencedirect.com/science/article/pii/S0167404816300013

Stefaniuk, T. 2020. Training in shaping employee information security awareness. Entrepreneurship and Sustainability Issues, 7(3), 1832-1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Tvaronavičienė, M., Plėta, T., Della Casa, S., Latvys, J. 2020. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. Insights into Regional Development, 2(4), 802-813. http://doi.org/10.9770/IRD.2020.2.4(6)

Vance, A., Siponen, M. T., & Straub, D. W. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management, 57(4), 103212. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0378720617307012

Zhang, D. (2018, October). Big data security and privacy protection. In 8th International Conference on Management and Computer Science (ICMCS 2018). Atlantis Press. Available at: https://www.atlantis-press.com/proceedings/icmcs-18/25904185

Short biographical note about the contributors at the end of the article:

Vladislav FEDORENKO, Doctor of Law, Professor, Director of the Research Center for Forensic Examination on Intellectual Property of the Ministry of Justice of Ukraine
ORCID ID: orcid.org/0000-0001-5902-1226

Nataliia LYTVYN, Doctor of Law, Professor, State Fiscal Service University of Ukraine
ORCID ID: orcid.org/0000-0003-4199-1413

Dmytro LUCHENKO, Doctor of Jurisprudence, Professor, Yaroslav Mudryi National Law University
ORCID ID: orcid.org/0000-0002-8666-2245

Iryna PANOVA, Ph.D. in Law, Associate Professor, Kharkiv National University of Internal Affairs
ORCID ID: orcid.org/0000-0003-4325-5428

Nelli TSYBULNYK, PhD in Law, Kharkiv National University of Internal Affairs
ORCID ID: orcid.org/0000-0002-5128-0511