JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2020 September Volume 10 Number 1
http://doi.org/10.9770/jssi.2020.10.1(13)

Scopus®

CYBERSECURITY AS AN ELEMENT OF FINANCIAL SECURITY IN THE CONDITIONS OF GLOBALIZATION

Oleksandr Ruvin[1]*, Nataliia Isaieva[2], Larysa Sukhomlyn[3], Kateryna Kalachenkova[4], Nataliia Bilianska[5]

*[1]*Kyiv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukraine, Smolenska Street, 6, Kyiv, 03057, Ukraine*
[2]V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine, Trohsvyatitelskaya Street, 4, Kyiv, 01001, Ukraine
[3]Kremenchuk Mykhailo Ostrohradskyi National University, 20, Pershotravneva Street, Kremenchuk, Poltava region, 39600, Ukraine
[4]Vasyl' Stus Donetsk National University 21, 600-richya str., Vinnytsia, 21021, Ukraine
[5]National Academy of Internal Affairs,1 Solomjanska Square, 03035, Kyiv, Ukraine

*E-mail: [1]*koaduep@gmail.com (Corresponding author)*

Received 11 January 2020; accepted 10 July 2020; published 30 September 2020

Abstract. The methodological foundations of the formation of analytical support for public administration of cybersecurity have been improved. Based on a combination of hierarchical and non-hierarchical clustering methods using the IBM SPSS Statistics package, the country's regions have been grouped into four clusters, which is the basis for adjusting the priorities of the state cybersecurity policy, a well-grounded approach when choosing means and instruments of influence at the regional level. In modern doctrine and practice of international law, the issues of qualification of cyber warfare remain controversial. There are approaches to justify the application of international humanitarian and criminal law. The most justified, in our opinion, is the qualification of cyber warfare as a violation of the UNO Charter and the use of force, and in some cases – the crime of aggression. The substantive rules of the institution of international cooperation in the fight against cybercrime determine the special principles of this kind of cooperation, the criminalization of certain types of illegal acts, as well as institutional mechanisms and capacity building. The system of international combating cybercrime is based on the principles of technical neutrality, multi-stakeholderism (public-private partnerships), as well as the equivalence of human rights online and offline. In the future, cybercrime will be associated with the use of innovative technologies. As it has been established by the example of the Internet of things, the latest technology, as a general rule, is included in the scope of existing international agreements on cybercrime, but there is no special regulation for them. We propose formal consolidation of the provision on "emergent technologies" in the texts of international legal acts in the field of combating cybercrime. First of all, this concerns the future UNO Convention on the fight against cybercrime, which should also provide for an additional body, such as the T-CY Committee under the Council of Europe Convention, which will provide clarification on the application of the agreement in specific changed circumstances.

Keywords: financial security, cybersecurity, cybercrime, Internet of things, information and communication technology.

Reference to this paper should be made as follows: Ruvin, O., Isaieva, N., Sukhomlyn, L., Kalachenkova, K., Bilianska, N. 2020. Cybersecurity as an element of financial security in the conditions of globalization. *Journal of Security and Sustainability Issues*, 10(1): 175-188. http://doi.org/10.9770/jssi.2020.10.1(13)

JEL Classifications: F35, F42

1. Introduction

The full functioning of society in modern conditions largely depends on information and communication technologies (hereinafter - ICT). Despite the positive achievements associated with the introduction of ICT, it must be noted that cyberspace is significantly criminalized. Statistics on the number of cybercrimes in the world are constantly growing, their consequences are becoming increasingly widespread, which indicates the need to

improve the existing system of combating cybercrime.

Given the special cross-border nature of this type of crime, the effectiveness of national mechanisms to combat cybercrime depends primarily on the effectiveness of the international legal cooperation of states in a certain area. In modern international law, there are rules aimed at regulating international relations in the fight against cybercrime, however, solutions to theoretical and practical problems associated with the creation of a universal concept of cybercrime, systemic mechanisms of international cooperation in this area remain on the agenda. In addition, it should also be taken into account that ICTs are developing at a very fast pace, therefore the regulatory framework, as well as scientific research, require constant modernization.

The aim of the work is a comprehensive analysis of international legal cooperation in the fight against cybercrime, a generalization of the basic principles of the universal concept of cybercrime, as well as determining the ways of its development.

2. Literature Survey

International and national legal acts, recognizing what cybercrime is, and what kind of acts are subject to criminalization, establish an appropriate framework for classifying crimes committed in cyberspace (Weber, R. H., & Studer, E. (2016)).

In the absence of universal international legal standards for determining the classification of cybercrimes, national criminal laws of states criminalize various types of illegal acts using ICT (McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016)).

However, an effective response to cybercrime, given its cross-border nature, is not possible if, due to inconsistency of the national criminal laws of individual states, the process of investigation, prosecution, or extradition of offenders is significantly complicated or excluded (Kent, A. D. (2016)).

In fact, these differences protect cybercriminals from prosecution, creating a kind of “barrier”, and provide an opportunity to avoid responsibility and punishment (Anwar, M., et al. (2017)).

Thus, the provisions of existing legal acts should provide an exhaustive list of cybercrimes in accordance with the nulla poena sine lege principle, and therefore the creation of relevant universal standards is an objective necessity (Do, C. T., et al. (2017)).

We conclude that in modern legal doctrine the definition of the concept of cybercrime remains a debatable issue. Conditionally existing approaches to understanding the phenomenon under study can be divided into the following groups.

1. Cybercrime is defined as the aggregate of crimes that infringe on computer systems and networks (Fielder, A., et al. (2016)).

2. Cybercrime is considered as a set of illegal acts, the objects of which are various types of information and ICT (Carr, M. (2016)) as means of implementation.

3. Cybercrime is understood as socially dangerous acts committed in cyberspace (Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017)).

The combination of all these characteristics, as well as the dynamic spread of computer technology and their development, lead to significant changes in law enforcement (Kurylo, M., Klochko, A., Zhuravlov, D., Javadov, H. (2018)).

Thus, from 30 to 70% of cybercrimes are transnational in nature, related to issues of conducting transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and the need for international cooperation (Maglaras, L. A., et al. (2018)).

Giving due to the academic improvement of work by scientists and despite a fairly high level of interest in issues related to the fight against cybercrime, insufficient attention has been paid to the analysis of international legal cooperation of states in a certain area, although the relevance of such a study is constantly growing.

3. Methods

The scientific validity of the conclusions drawn is determined by the set of methods of scientific knowledge.

Logical-semantic and linguistic methods provided the opportunity to study in-depth the conceptual-categorial apparatus. Using the historical and legal method, the genesis and stages of development of the institution of international cooperation of states in the fight against cybercrime, the stage of formation of national legislation in the field of combating high-tech crime were investigated. The analysis of many international and domestic legal acts was based on the use of the formal legal method.

The information base is the materials of the Ministry of Internal Affairs, the Department of Cyber Police of the National Police of Ukraine, the State Statistics Committee of Ukraine, Eurostat, international companies in the field of information security, the work of scientists, as well as the results of the author's own research.

The normative and empirical basis of the study is made up of international treaties, decisions of international intergovernmental organizations, and legal acts of states.

4. Results

The increase in the penetration and use of the Internet and social media by individuals, enterprises, and government agencies not only promote development, provide opportunities for the development of new areas of activity but also pose a threat to increasing vulnerability in computer networks and increasing the risk of cyber incidents.

These trends have a direct impact on the formation and implementation of the state policy of ensuring cybersecurity. Therefore, their monitoring and permanent analysis are becoming crucial for ensuring national security in modern conditions.

International cooperation of states in the fight against cybercrime on an ongoing basis is carried out within the framework of various international organizations. Building an effective institutional system of international cooperation in the fight against cybercrime is an important direction in the regulation of a certain area (Drobyazko, S., et al. (2019a), Drobyazko, S., et al. (2019b); Korauš et al., 2019; Ključnikov et al., 2019; Plėta et al., 2020).

Most international organizations create separate units to ensure cooperation between states in combatting cybercrime. Due to such a haphazard formation of various institutions, duplication of functions and powers often occurs, and on the other hand, the effectiveness of such an inconsistent mechanism is reduced. Let's consider the existing mechanisms of cooperation between states to counter cybercrime in more detail.

The United Nations, in particular the General Assembly, the Economic and Social Council, the UN Secretariat, as well as specialized agencies, are central to this mechanism. Special functions to combat high-tech crime are assigned to the United Nations Office on Drugs and Crime (UNODC), which runs the Global Program on Cybercrime (GPC), as well as the Open-ended Intergovernmental Expert Group on Cybercrime. UNODC promotes long-term and sustainable capacity-building in the fight against cybercrime by supporting national structures and actions.

Paying attention to the level of cybersecurity, you should pay attention to the information on the National Cybersecurity Index (NCSI) - a global index that measures the willingness of countries to prevent the imple-

mentation of fundamental cyberthreats, managing cyber incidents, crime and large-scale cybercrisis (Global Cybersecurity Index 2018).

The index is evaluated by the following groups of indicators that contain indicators:

1. General indicators of cybersecurity:

cybersecurity policy development (cybersecurity policy unit; cybersecurity policy alignment format; cybersecurity strategy; plan for implementing the cybersecurity strategy)

analysis and information on cyberthreats (cyberthreats analysis unit; public reports on cyberthreats are published annually; cyberspace safety and security website)

education and professional development (cybersecurity competencies in primary or secondary education; bachelor-level cybersecurity program; master's cybersecurity program; Doctor of Science level cybersecurity program and professional cybersecurity association)

contribution to global cybersecurity (convention on cybercrime; representation in the formats of international cooperation; international organization on cybersecurity, which the country accepts, increase in the potential of cybersecurity for other countries).

2. Business security indicators: protection of digital services; protection of basic services; electronic identification and trust services; protection of personal data.

3. Performance management and crisis indicators: response to cyber incidents; cyber crisis management; fight against cybercrime; military cyber operations.

In 2018, according to this index, Ukraine ranked 26th out of 131, which indicates a fairly high performance of the country's ability to develop a national cyber defense policy, the ability to fight cybercrime, and provide electronic identification and electronic signature services (Table 1).

Table 1. Top 30 countries according to the National Cybersecurity Index (2018)

Place	Country	Index Value	Place	Country	Index Value	Place	Country	Index Value
1	Czech Republic	90,91	11	Singapore	80,52	21	Georgia	64,94
2	Estonia	90,91	12	Slovakia	79,22	22	Hungary	64,94
3	Spain	89,61	13	Italy	76,62	23	Russia	64,94
4	Lithuania	88,31	14	United Kingdom	75,32	24	Belgium	64,94
5	Greece	87,01	15	Malaysia	72,73	25	Israel	64,94
6	France	83,12	16	Switzerland	72,73	26	Ukraine	63,64
7	Finland	81,82	17	Romania	71,43	27	Serbia	63,64
8	Denmark	81,82	18	Latvia	71,43	28	Ireland	63,64
9	Netherlands	81,82	19	Poland	70,13	29	USA	63,64
10	Germany	80,52	20	Portugal	68,83	30	Japan	62,34

Source: Designed by the author according to the Global Cybersecurity Index 2018

The results of research on the development of the Internet in Ukraine show that 60.7% of the country's population (25.59 million people) are its users. At the same time, 42% of the population (18.7 million people) use mobile Internet, 29% (13 million people) use social networks, of which 22% of the population (9.5 million) access social networks via mobile phone (Table 2).

Table 2. Use of the Internet and population statistics in Ukraine (2018)

Year	Population number, persons	Internet users		
		Number of people	penetration rate (% of the population)	growth rate 2000-2018,%
2000	49084600	200000	0,4	X
2006	45833977	5278100	11,5	2639,05
2010	45415596	15300000	33,7	289,87
2018	42153200	25590000	60,7	167,26

Source: Designed by the author according to Digital 2018 Ukraine

It should be noted that global trends of increasing the penetration level, use of the Internet and social media by individuals and companies are typical for Ukraine, which, in turn, contributes to the development of Internet business. These facts have been confirmed in a number of studies.

Thus, in 2017, the total cost of purchasing goods through electronic platforms amounted to 1.474 trillion dollars, which is 16% more than in 2016 (Digital 2018 Ukraine).

These dynamics have forever changed user behavior, as ordinary citizens and business professionals are increasingly conducting research, making purchasing decisions, seeking support, and recommending brands online.

It should be noted that the most important changes in the digital sphere are expected in the near future: audiovisual content will begin to prevail over text; social relations and online societies will develop in such a way as to adopt these new ways of human interaction.

According to the study World Economic Research crimes and fraud in 2018: results of the Ukrainian survey organizations. Removing fraud from the shadows, cybercrime is one of the five main types of economic crimes and (or) fraud in 2018 (Figure 1).

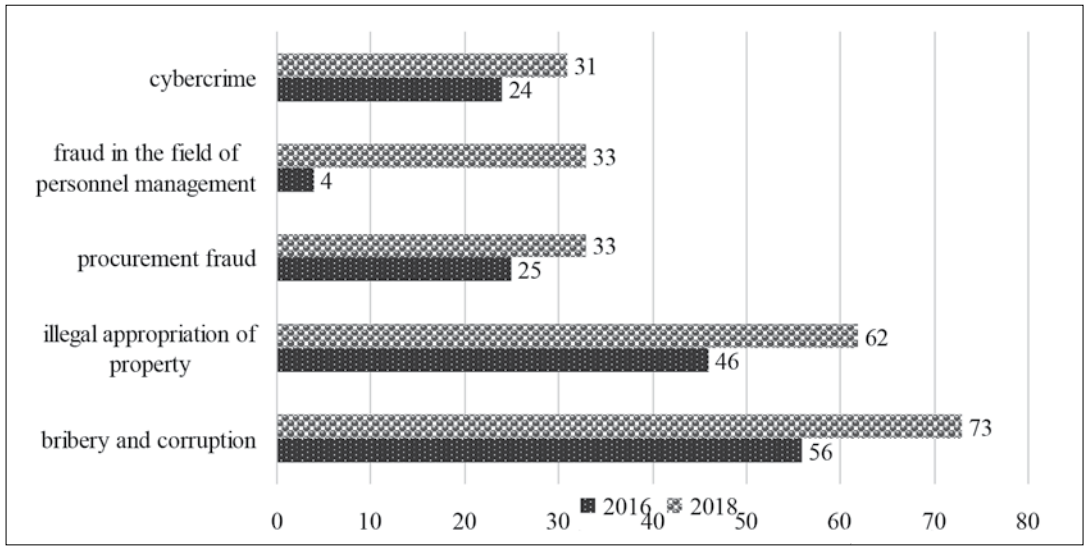

Figure 1. TOP 5 main types of economic crimes and (or) fraud at Ukrainian enterprises and organizations in 2016 and 2018, %

Source: Designed by the author according to the data of the World Economic Research crimes and fraud in 2018: results of the Ukrainian survey organizations. Removing fraud from the shadows

According to the survey (2018), the number of cybercrimes that enterprises and organizations face in Ukraine is growing by 7% compared to 2016, causing high risks for both various sectors of the national economy and for the public administration sphere.

From this type of crime, which has become one of the most common types of economic atrocities, taking 5th place among types of fraud, 31% of Ukrainian enterprises and organizations suffered, which is fully consistent with global sad trends (31% of respondents and 5th place).

At the same time, the development of technologies has led to a number of new threats for organizations, including: malware, phishing, network scanning, and password-guessing attacks.

It should be noted that more than a third of Ukrainian organizations subjected to cyber attacks affected by the consequences of malicious software. As a result of cyberattacks, not only the business processes of organizations (51%) were violated but also the significant losses caused (Figure 2).

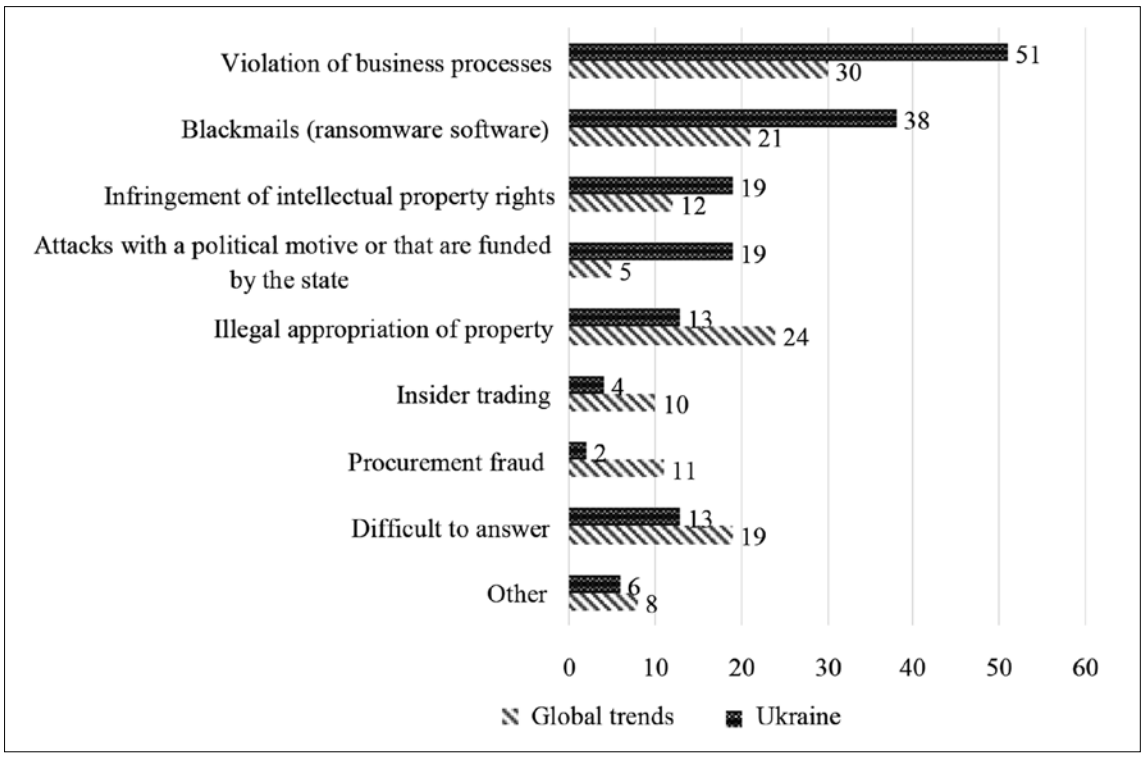

Figure 2. TOP 5 main types of economic crimes and (or) fraud at Ukrainian enterprises and organizations in 2018, %

Source: Designed by the author according to Ukraine Worldwide Review economic crimes. Cybercrime in the center attention (2011)

It should be noted that, in 2018, 16% determined the probability that their organization will suffer from cybercrime in the next two years, which indicates the feasibility of paying maximum attention to this type of economic crime at the level of enterprises of various forms of ownership and activities as well as at the level of formation of effective state policy.

Thus, it should be noted that the number of crimes in the use of electronic computers, systems and computer networks, and telecommunications networks have been growing steadily since 2014, reaching 2573 crimes in 2017 (Figure 3). The growth rate for 2014-2017 was 480.8%. For 8 months of 2018, this figure has already exceeded the level of 2016 by 117.9%.

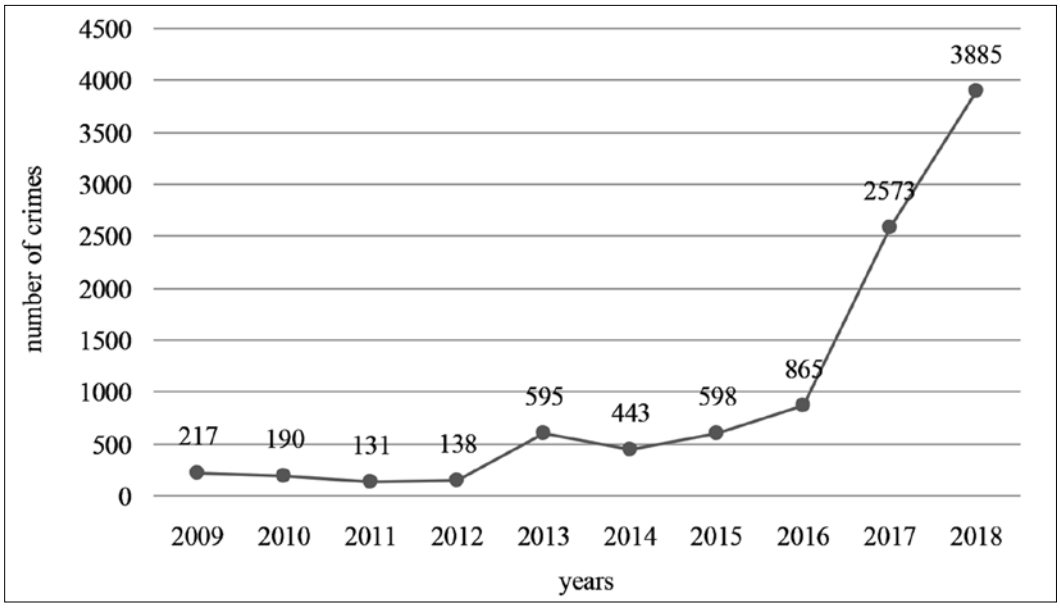

Figure 3. Dynamics of reported cybercrime in Ukraine, the number of crimes

Source: Designed by the author according to Criminal Statistics Report in Ukraine (2019)

These trends have developed under the influence of a number of factors. Among the main ones are the following: significant pace of informatization of society; technical backwardness of the law enforcement system and the need to reform it; insufficient funding for cybersecurity measures.

The outstripping growth of registered cybercrimes has led to an increase in their share in the total number of crimes in Ukraine, maintaining trends of increase from 0.08% in 2014 to 0.51 in 2018, which is the highest figure since 2009 (Figure 4).

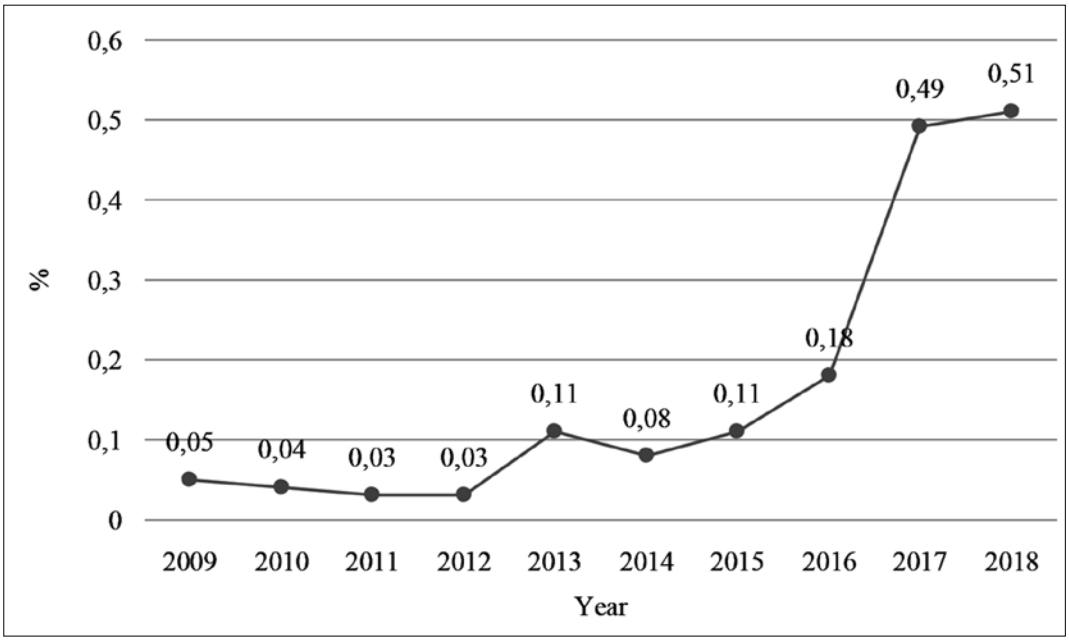

Figure 4. The share of cybercrime in the total number of crimes registered in Ukraine in the dynamics, %

Source: Designed by the author according to Criminal Statistics Report in Ukraine (2019)

According to 2018, police officers exposed more than 800 people who were involved in crimes in the field of high information technology. According to statistics, most of the suspects are men aged 25 to 40 (Table 3).

Table 3. Distribution of cybercriminals by sex, % (according to 2018)

Age	Men	Women
Together, of them:	67	33
Up to 25 years	13	6
25-40 years	39	20
40 and more	15	7

Source: Designed by the author according to Cyberpolice Department of the National Police of Ukraine

Analysis of the structure of cybercrime by type shows that, at the same time, in the field of cybersecurity the largest number of users of malicious software who committed crimes using viruses purchased on DarkNet were found (Figure 5).

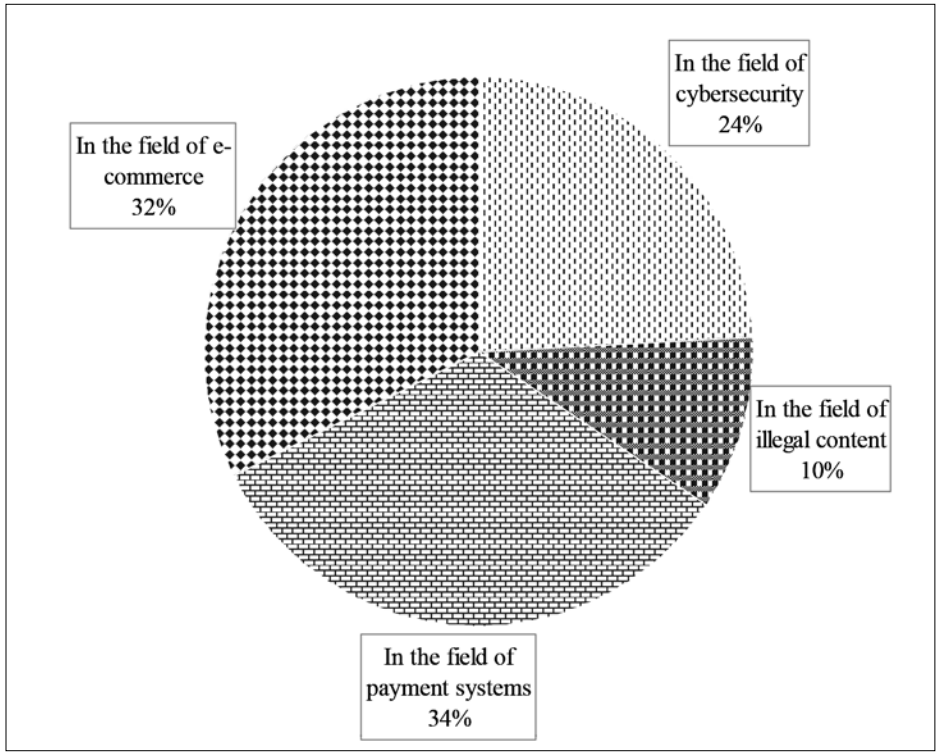

Figure 5. Structure of detected cybercrimes by type (according to 2018), %

Source: Designed by the author according to Cyberpolice Department of the National Police of Ukraine

It should be noted that in order to detect cybercrime, the Ukrainian cyberpolice develops and implements in practice the modern methods of detecting, recording, and investigating digital evidence. In particular, during 2018, 5.5 petabytes of information were examined and analyzed by cyber police experts, which was subsequently identified as digital evidence. Based on the results of international cooperation, in 2018, 8 transnational hacker groups were discovered and more than 30 international operations were conducted.

It should be noted that in 2018, agreements on cooperation in the fight against cybercrime were signed with organizations of both the public and private sectors. Among them are representatives of international campaigns in the field of information security and IT companies, the police of Australia, Singapore, Qatar, and other countries. In addition, effective interaction has been established with the most famous world social networks.

The growing informatization of the country and the increasing pressure of cyber influences actualizes the role of the state and relevant state regulation in ensuring cybersecurity. This is due to the fact that it is the state that determines the policy of national security, sustainable development, digitalization of the economy, etc.

The analysis showed that the number of cybercrimes in Ukraine is growing at a faster pace, while the law enforcement system was technically not ready to prevent them.

Thus, the problem of attracting and optimizing the technical, financial, and organizational and managerial resources, which are necessary to effectively overcome cybercrime in Ukraine today, is becoming one of the main tasks of the state policy of ensuring cybersecurity and is an integral part of national security policy.

For the practical implementation of the clustering process, the statistical package IBM SPSS Statistics was used.

The main stages of the clustering process are as follows:

based on hierarchical cluster analysis, the optimal number of clusters was established - 4;

based on the k-means method, division into clusters is carried out.

It should be noted that according to the results of clustering based on the distribution of the regions of Ukraine according to the level of cyberthreats, four clusters are identified:

the first cluster - with a very high level of cyberthreats - Lugansk and Chernihiv regions (with an average value of the integral indicator for assessing the level of cyberthreats 7.022 and 6.234, respectively);

the second cluster includes four regions with a high level of cyberthreats. These are Chernivtsi, Kherson, Zhytomyr, and Khmelnytskyi regions (the limit values of the integral indicator are from 4.327 to 5.216)

The cluster 3 combines regions with an average level of cyberthreats and includes seven regions with integral indicators - from 2,491 to 4,013.

The cluster 4 is represented by twelve regions (the value of the integral indicator is from 1.083 to 2.194 (Table 4).

Table 4. Results of clustering of regions of Ukraine by the level of cyberthreats (according to 2018)

No. of the cluster	Name of the cluster	Region	Value of the integrated indicator for assessing the level of cyberthreats
1	Regions with a very high level of cyber threats	Luhansk	7,022
		Chernihiv	6,234
2	Regions with a high level of cyber threats	Khmelnytsky	5,216
		Zhytomyr	4,826
		Kherson	4,751
		Chernivtsi	4,327
3	Regions with an average level of cyber threats	Cherkasy	4,013
		Rivne	3,708
		City of Kyiv	3,702
		Volyn	3,197
		Sumy	3,076
		Kirovograd	2,851
		Transcarpathian	2,491

4	Regions with a level of cyber threats below average	Mykolayivska	2,194
		Ternopil	1,755
		Poltava	1,658
		Ivano-Frankivsk	1,499
		Odessa	1,344
		Donetsk	1,303
		Zaporozhye	1,253
		Kharkiv	1,164
		Kyiv	1,158
		Dnepropetrovsk	1,146
		Lviv	1,086
		Vinnytsia	1,083

Source: Calculated by the author using the IBM SPSS Statistics package

Confirmation of the theoretical assumption about the relationship between the number of recorded criminal offenses in the use of electronic computers, systems and computer telecommunication networks and the integrated indicator for assessing the level of cyber threats has led to the conclusion that it is necessary to create effective tools and implement measures aimed at combating crime in cyberspace.

The proposed methodological foundations for the formation of analytical support for cybersecurity management, which provide an integrated assessment of the level of cyber protection of the country's regions and their distribution into clusters, are the basis for substantiating the directions of the state cybersecurity policy.

Further analysis of the results is the basis for adjusting the directions of the state cybersecurity policy and differentiating the means of influence at the regional level.

In addition, it should be noted that one of the problems in the field of cyber defense is that Ukraine (especially the telecommunication component of its information infrastructure) is still fundamentally vulnerable to cyber threats and not least because of the overly excessive broadcasting of foreign software products and the use of the material and technical base of foreign production.

The search for possible "bookmarks" in these products is practically impossible due to the state's dependence on the products mentioned, which has reached a level that really threatens national security in all areas.

In this regard, having examined the situation, the complex of problems in the field of cybersecurity and the level of threats to national security, the National Security and Defense Council of Ukraine (NSDC of Ukraine) identified a number of measures aimed at increasing the effectiveness of countering relevant cyber threats and responsible entities.

Among the most important of them, the following are highlighted: to immediately prepare legislative proposals to determine the mechanism of interaction between cybersecurity entities and owners (managers) of critical information infrastructure objects during the detection, prevention, and suppression of cyber attacks and cyber incidents; to ensure the preparation of legislative proposals to strengthen the responsibility for failure to comply with the requirements of the legislation on the protection of information in information and telecommunication systems; to ensure the creation of unified primary and backup secure data centers for storing information of state electronic information resources; to work out the issue of stimulating the development and implementation of software for the needs of state authorities and other state bodies, enterprises, institutions and organizations of state ownership, and the like.

Thus, in the process of the study, we come to the following conclusions. Substantive rules constitute a separate part of the structure of the institution of international legal cooperation in the fight against cybercrime. Using

these norms, the general principles of international legal cooperation of states in the fight against cybercrime, the criminalization of certain types of illegal acts, as well as the determination of the institutional framework of international cooperation and capacity building in the field of combating cybercrimes are established.

The Institute of International Legal Cooperation in the Field of Combating Cybercrime is subject to the basic principles of law and certainly spreads its influence in cyberspace (Karpenko, L., et al. (2018); Tetiana, H., et al. (2019); Chechel, A. et al. (2020)).

Thus, there is a consistency of international anti-cybercrime standards with the basic principles of international law. On the other hand, one can objectively assert about the formation of a system of special principles of the institute under study. So, they should include:

- the principle of technical neutrality, which means an equal assessment of technologies in the system of combating cybercrime, prohibiting any priority among them;
- the principle of multi-stakeholderism (or public-private partnership), which means involving all interested parties in the fight against cybercrime, including non-state ones;
- the principle of the equivalence of human rights online and offline, which means the obligation to protect human rights in cyberspace along with physical space, including in the fight against cybercrime.

High-tech crime in the future will be associated with such innovations as Artificial Intelligence, Cloud Technology, Internet of Things (hereinafter IoT), Data grid, Distributed Ledger Technology (hereinafter - DLT), and Blockchain. For example, the Internet of things - as a phenomenon based on the top of the existing Internet infrastructure, significantly expands the virtual

For example, the Internet of things, as a phenomenon based on the top of the existing Internet infrastructure, significantly expands the virtual environment of opportunities for cybercriminals. The number of connections and nodes, which exist simultaneously throughout the world, is growing, control over which is actually decreasing. Thus, IoT, together with other ICTs, acts as a means of implementing high-tech crime or an object of criminal encroachment. In addition, there are growing opportunities to conceal crimes committed using IoT. Using the technology of the Internet of things as an example, it was found that innovative technologies, as a general rule, fall within the scope of existing international agreements on cybercrime. However, there is no special regulatory provision.

Since the development of security for innovative technologies, including the Internet of Things, is an important element in building a preventive cybercrime system, we propose to improve the existing substantive regulation of international cybercrime counteraction by including provisions on “emergent technologies”. As a result, the scope of international legal cooperation of states in the fight against cybercrime will extend to any innovative technology. This statement must be formalized into a general rule, and additionally interpreted by a specially defined body, such as the T-CY Committee, in accordance with the Convention on Cybercrime of the Council of Europe.

5. Discussion

In the system of modern international law, there are a significant number of international legal acts aimed at regulating international cooperation in the fight against cybercrime. Together, they form the institution of international legal cooperation in the fight against cybercrime. This is a set of material and procedural norms and principles that govern cooperation between states aimed at combating cybercrime.

The specified institution is at the formation stage and is being implemented at the supranational level within the framework of international legal assistance and cooperation in criminal matters. The institute under study is characterized by fragmentation and heterogeneity, which requires coordination and harmonization. To this end, the development and adoption of a universal international treaty within the framework of the United Na-

tions is necessary. For these reasons, we consider it appropriate to initiate the preparation of a universal UNO Convention against Cybercrime.

The lack of a formally expressed consensus of states and the doctrinal uncertainty regarding the qualification of cyber warfare under international law leave it open for discussion. In these circumstances, the process of deepening the information confrontation between states, the militarization of cyberspace, the development of cyber weapons, and the buildup of cybernetic capacities and tactics as a national resource of states occur. In positive law, there is no precautionary measure to protect the weak side in the application of information impact methods. Consequently, the only way out for states is to defend and launch cyber attacks in response.

In modern doctrine and practice of international law, there are two possible approaches to qualifying cyberattacks, which can mean cyber warfare. On the one hand, provided that they meet criteria such as:

1) the qualification of cybernetic means as a military force or military violence;

2) the implementation of cyber attacks by states or organized armed groups, they may be subject to international humanitarian law.

Within the virtual space, not only borders are dissolved but also the difference between military goals and peaceful objects (including cultural values, critical infrastructure, etc.), between the military and civilians is dissolved.

On the other hand, cyber attacks can be qualified as a crime of aggression under international criminal law. Such a decision should be considered in each case, assessing the nature, gravity, and scale of the violation of the UNO Charter.

Thus, we consider the most justified recognition of cyber warfare as an act of the use of force in accordance with the UNO Charter and in some cases - crimes of aggression.

An effective fight against local cybercrime of a content nature can serve as a factor in the prevention of international conflicts and cyberwarfare.

Conclusions

The basic statistical indicators characterizing the level of use of information and communication technologies at enterprises and organizations of Ukraine are analyzed, which made it possible to ascertain the increase in the number of computer equipment, increased access to the Internet, and an increase in the level of use of information and communication technologies.

It was established that these trends created not only prerequisites for the development of enterprises and the national economy as a whole but also caused an increase in crime in this area. It is noted that in order to detect cybercrime, cyber police developed and implemented modern methods of detecting, recording, and studying digital evidence.

The role of the state in ensuring cybersecurity has been actualized. The attention is focused on the fact that, from the point of view of developing an effective cybersecurity system, the regulatory framework for its introduction, which is represented by international and national regulatory legal acts, is fundamental.

The improvement of the material standards of the institution of international legal opposition to cybercrime occurs in relation to crimes related to illegal content. Due to the close relationship between the prohibition of the creation and dissemination of illegal information and human rights, it is permissible to criminalize only extreme forms of expression, which must meet the requirements of proportionality, expediency, and legality. Such a prohibition should also be objectively determined by the needs of protecting human rights, ensuring the rule of law, and the rule of law and security.

Measures of established liability for the dissemination of prohibited information cannot exceed the level of potential harm that these data and access to it can cause. An exhaustive list of information, which is illegal, has not been established by international agreements. Modern international law criminalizes only foolishness or the justification of genocide or other crimes against humanity and propaganda for war, which constitute the obligations of erga omnes, as well as any actions related to child pornography and racist or xenophobic material. We consider a positive trend towards increased responsibility of intermediaries (such as social networks and search resources) who exercise control and can influence the content of the information distributed.

To implement a common policy in the fight against cybercrime, as well as building capacity, states have intensified cooperation in many institutional mechanisms, both universal and regional. However, it should be noted that the competencies of these institutions are predominantly duplicated. We believe that, as a result of this, the effectiveness of international cooperation between states to combat cybercrime is inevitably reduced. Moreover, institutional mechanisms in the field of combating high-tech crime are created in the absence of sufficient conventional mechanisms, primarily a universal international treaty on cybercrime. As a result, in the new regions, additional cybercrime centers are forming or existing ones are artificially expanding.

References

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43-62. https://doi.org/10.1111/1468-2346.12504

Chechel A., Ilyina A., Orlova N., Fayvishenko D., Kulchil I., Pidlisna T. (2020). Human Capital Development in the Process of the Use and Provision of Electronic Services in Ukraine // 35th IBIMA Conference: 1-2 April 2020, Seville, Spain. URL: https://ibima.org/accepted-paper/human-capital-development-in-the-process-of-the-use-and-provision-of-electronic-services-in-ukraine/

Criminal Statistics Report in Ukraine (2019). Available at: https://rpr.org.ua/wp-content/uploads/2019/09/1568808134cplr.-report-on-criminal-statistics-in-ukraine.pdf

Cyberpolice Department of the National Police of Ukraine. URL: https://cyberpolice.gov.ua/results/2018/

Digital 2018 Ukraine. Available at: https://www.slideshare.net/DataReportal/digital-2018-ukraine-january-2018

Do, C. T., Tran, N. H., Hong, C., Kamhoua, C. A., Kwiat, K. A., Blasch, E., ... & Iyengar, S. S. (2017). Game theory for cyber security and privacy. ACM Computing Surveys (CSUR), 50(2), 1-37. https://doi.org/10.1145/3057268

Drobyazko, S., Blahuta, R., Gurkovskyi, V., Marchenko, Y., Shevchenko, L. (2019). Peculiarities of the legal control of cryptocurrency circulation in Ukraine. Journal of Legal, Ethical and Regulatory Issues. Vol: 22 Issue: 6. URL: https://www.abacademies.org/articles/peculiarities-of-the-legal-control-of-cryptocurrency-circulation-in-ukraine-8813.html

Drobyazko S., Makedon V., Zhuravlov D., Buglak Y., Stetsenko V. (2019) Ethical, Technological and Patent Aspects of Technology Blockchain Distribution. Journal of Legal, Ethical and Regulatory Issues. Vol: 22 Issue: 2S. URL: https://www.abacademies.org/articles/ethical-technological-and-patent-aspects-of-technology-blockchain-distribution-8434.html

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. Decision support systems, 86, 13-23. https://doi.org/10.1016/j.dss.2016.02.012

Global Cybersecurity Index 2018. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Karpenko, L., Serbov, M., Kwilinski, A., Makedon, V., & Drobyazko, S. (2018). Methodological platform of the control mechanism with the energy saving technologies. Academy of Strategic Management Journal, 17(5), 1939-6104-17-5-271: 1-7. Retrieved from https://www.abacademies.org/articles/Methodological-platform-of-the-control-mechanism-1939-6104-17-5-271.pdf

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)

Korauš, A., Gombár, M., Kelemen, P., Polák, J. (2019). Analysis of respondents' opinions and attitudes toward the security of payment systems. Entrepreneurship and Sustainability Issues, 6(4), 1987-2002. http://doi.org/10.9770/jesi.2019.6.4(31)

Kurylo, M., Klochko, A., Zhuravlov, D., Javadov, H. (2018). Economic and legal aspects of banking security under European integration intensification in Ukraine. Banks and Bank Systems 13(1), 162-172. Available at: http://nbuv.gov.ua/UJRN/banks_2017_13_1_17

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., ... & Cruz, T. J. (2018). Cyber security of critical infrastructures. Ict Express, 4(1), 42-45. https://doi.org/10.1016/j.icte.2018.02.001

McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R. (2016). The cybersecurity landscape in industrial control systems. Proceedings of the IEEE, 104(5), 1039-1057. Available at: https://ieeexplore.ieee.org/abstract/document/7434576

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication, 800(2017), 181. Available at: https://www.schoolofcybersecurity.com/wp-content/uploads/2018/04/NIST.SP_.800-181.pdf

Plėta, T., Tvaronavičienė, M., Della Casa, S. (2020)**.** Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development,* 2(2), 538-548. https://doi.org/10.9770/IRD.2020.2.2(3)

Tetiana, H., Chernysh O., Levchenko, A., Semenenko, O., Mykhailichenko H. (2019). Strategic Solutions for the Implementation of Innovation Projects. Academy of Strategic Management Journal. Volume 18, Special Issue 1. Available at: https://www.abacademies.org/articles/Strategic-solutions-for-the-implementation-of-innovation-projects-1939-6104-18-SI-1-444.pdf

Ukraine Worldwide Review economic crimes. Cybercrime in the center attention (2011). Available at: https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 32(5), 715-728. https://doi.org/10.1016/j.clsr.2016.07.002

World Economic Research crimes and fraud in 2018: results of the Ukrainian survey organizations. Removing fraud from the shadows. Available at: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf

Oleksandr RUVIN, Ph.D. in Law, Director, Kyiv Scientific Research Institute of Forensic Expertise of the Ministry of Justice of Ukrain
ORCID ID: orcid.org/0000-0003-4752-1278

Nataliia ISAIEVA, PhD in Law, Associate Professor, Senior Scientific Reseacher V.M. Koretsky Institute of State and Law of National Academy of Sciences of Ukraine
ORCID ID: orcid.org/0000-0002-9716-9472

Larysa SUKHOMLYN, Candidate of Engineering Sciences, Associate Professor, Kremenchuk Mykhailo Ostrohradskyi National University
ORCID ID: orcid.org/0000-0001-9511-5932

Kateryna KALACHENKOVA, PhD in Law, Associate Professor, Vasyl' Stus Donetsk National University
ORCID ID: orcid.org/0000-0003-0720-2476

Nataliia BILIANSKA, PhD in Law, Associate Professor, National Academy of Internal Affairs
ORCID ID: orcid.org/0000-0002-1650-5500

Register for an **ORCID ID**:
https://orcid.org/register