Advances in Social Science, Education and Humanities Research, volume 217
2nd International Conference on Social, economic, and academic leadership (ICSEAL 2018)

Cybercrime as a leading threat to information security in the countries with transitional economy

Mykola Syomych
Poltava State Agrarian Academy
Skovorody str. 1/3, 36000, Poltava
Ukraine
e-mail: SNI50@ukr.net

Iryna Markina
Poltava State Agrarian Academy
Skovorody str. 1/3, 36000, Poltava
Ukraine
e-mail: iriska7@ukr.net

Dmytro Diachkov
Poltava State Agrarian Academy
Skovorody str. 1/3, 36000, Poltava
Ukraine
e-mail: dmiraf@ukr.net

Abstract The peculiarity of the modern economy is related to its informational character which affects the sharp increase of cyber incidents in the field of information security that are widespread and becoming threatening and are relevant to a broad range of private, corporate, as well as state interests. The problem of forming an effective information security system is exacerbated by the spread of cybercrime as a leading threat to information security, both in Ukraine and throughout the world. Thus, World Economic Crime Survey shows that almost every third organization faces economic offenses, of which about a third are the cybercrimes.
The paper analyzes the data of two main indicators of the country's cybersecurity: Global Cybersecurity Index and the National Cybersecurity Index. According to the first one, some indicators of the Index in contemporary Ukraine became problematic. These are as follows: the absence of sectoral cybersecurity centers, the lack or low standards of cybersecurity of organizations and professional standards in this field, Internet safety for children, and the practical implementation of activities. The results of the analysis of the main indicators of the National Cybersecurity Index make it possible to state that the leading shortcomings in the field of cyber defense for Ukraine are: the lack of protection of digital services, the lack of crisis management in the field of cyber crisis management, the lack of effective military cyber operations. Summarizing the foregoing, the most acute problems of ensuring the proper level of cyber security of Ukraine are identified, which are as follows: the lack of appropriate specialists in the field of cybersecurity, the lack of unification of the categorical apparatus in the legislation of the country in the field of cybercrime, the lack of standards of cybersecurity in organizations and professional standards in this field, the absence of sectoral cybersecurity centers, the lack of recognized national comparative analysis and reference for measuring cybersecurity, and finally, the severity of identification, investigation and disclosure of cybercrime. In order to overcome certain shortcomings, the conceptual ways of solving the problem of ensuring cybersecurity have been proposed and characterized, which mainly consist in improving the legal and organizational support for the information and cyber security of Ukraine.

1 Introduction

Rapid globalization of our society contributes to the growth of the role of information security for the international community, as well as for the state, and the various sectors of the economy, enterprises and individuals. In the conditions of the development of the knowledge economy, knowledge-intensive industries and information technologies that make up the priority sector of economic development come to the forefront. With rational regulation, this sector can bring the state, industry, enterprise and personality to a qualitatively new level of development (Olshanska 2015; Lisin et al. 2015; Zielińska 2016; Oláh et al. 2017; or Bychkova et al. 2018).

A feature of the modern economy is its transformational and at the same time informational character, the computerization of managerial and production processes, the automation of control systems, the use of technical means of communication and data transmission networks, digital cloud technologies, as well as the use of digital

data. In this regard, in the field of information technology, the risk of information loss and theft increases with mobility (Čábelková et al. 2015; or Moyseyenko and Ryvak 2016). Consequently, the actual task for the state as a whole and for business entities in particular, is to ensure their information security (Pusak and Marchenko 2018; Naumov et al. 2018; Markina 2016; or Shvetsova et al. 2018).

At present, there is a sharp increase of incidents in the field of information security that are widespread and becoming threatening and are relevant to a broad range of private, corporate, and state interests. The main trends in the development of the above-mentioned threats are the following ones:

- an increase in the number of cyberattacks, many of which lead to significant losses;
- an increase in the complexity of cyberattacks, which may include several stages and apply special methods of protection against possible countermeasures;
- the impact of cyberattacks on the majority of electronic (digital) devices;
- an increase in the number of cyberattacks on the information infrastructure of large corporations, important industrial sites and even state structures;
- the use of various means and methods of cyber attacks on the state by the most developed countries in the field of computer technology.

Consequently, the problem of forming an effective information security system is exacerbated by the spread of cybercrime as a leading threat to information security, both in Ukraine and throughout the world.

The problem of cybersecurity in general, and the system of its ensuring, in particular, because of its specificity, is global and not isolated. So it can be effectively solved only under the condition of coordinated activity of subjects of cybersecurity. Therefore, to ensure effective interaction at the international level, a coherent understanding of the issues of "ensuring cybersecurity" is necessary.

The majority of specialists in the subject area under study consider the ensuring of information and cybersecurity from the standpoint of an organizational or technical and technological approach that envisages the existence of a management system and the necessary technology and software of information security (Kolesnik et al. 2003; Kavun and Golubev 2013; Markina 2016; Finance UA 2017; or Marutian 2017). At the same time, the initial hypothesis of the proposed study is the interdependence between the complex approach of the subjects of different levels of management to ensuring adequate information security conditions (in particular cybersecurity), and the availability of the necessary organizational and legal support for it at the micro and macro levels.

2 Literature review

According to the PWC Global Economic Crime Survey held in 2016, almost every third organization has already faced economic offenses, of which about a third (32%) were related to cybercrimes (PwC 2016). According to the PsC's "Global State of Information Security Survey", cybercrime as early as 2011 was one of the five most common economic crimes in Ukraine (PwC 2018). The survey data that was conducted among top-level specialists and managers, which carry out research and work in 13 main sectors of the economy, make it possible to determine that:

- every third respondent (37%) believes that the risk of cybercrime is increasing annually;
- more than 25% of the organizations surveyed reported that they do not have the appropriate security policies and mechanisms for responding to cybercrime;
- 46% of respondents did not study cybersecurity in the last 12 months;
- 58% of respondents from Ukraine stated that in their organizations there is no monitoring process of social networking visits (Ukraine. World Economic Crime Review. Cybercriminals are at the center of attention).

The statistics of the Ministry of Internal Affairs of Ukraine and the Prosecutor General's Office of Ukraine testify to the rapid growth of cybercrime during the last decade. Thus, for example, in 2005-2009, there was a general tendency to increase the number of crimes in the field of information technology: in 2005 only 615 crimes were identified, and in 2009 – there were 707 crimes identified. Since 2010, the statistics of crimes in the sphere of the use of electronic computers (computers), systems and computer networks and telecommunication networks is conducted in Ukraine. In 2010, about 190 crimes of this nature were registered, in 2011 there were only 131 of them, and in 2017 there were already 2,573 crimes related to this sphere (MBC 2018). According to the information provided by the Prosecutor General's Office of Ukraine, the largest number of such crimes is registered in Lviv, Mykolayiv, Odesa, Volyn and Chernivtsi regions and in the city of Kiev (See Table 1).

Table 1. Registered crimes in the field of the use of electronic computers (computers), systems and computer networks and telecommunication networks (2016)

Region	Registered	Criminal offenses in which the proceedings are closed		Criminal offences accounted for* in the reporting period	Criminal offenses for which the proceedings are submitted to the Court **	Criminal offenses in which at the end of the reporting period the decision is not taken (on termination or suspension)
		Total	Including part 1 of paragraphs 1, 2, 4, 6 of Article 284 of the Code of Criminal Procedure of Ukraine			
Autonomous Republic of *Crimea*	**1**	0	0	1	0	0
Vinnytsya region	**25**	2	2	23	4	20
Volyn region	**75**	2	2	73	65	9
Dnipropetrovsk region	**39**	10	10	29	2	13
Donetskregion	**10**	1	1	9	1	8
Zhytomyrregion	**9**	0	0	9	2	7
*Zakarpatskyi*region	**7**	2	2	5	4	4
Zaporizhzhya region	46	1	1	45	5	23
Ivano-Frankivskregion	**25**	2	2	23	19	6
Kyivregion	**31**	2	2	29	3	28
Kirovograd region	**20**	1	1	19	10	9
Luhanskregion	**2**	0	0	2	0	2
Lvivregion	**150**	8	8	142	117	25
The city of Kyiv	**155**	43	43	112	17	98
The city of Sevastopol	**0**	0	0	0	0	0
Mykolayiv region	**130**	9	9	121	91	30
Odesaregion	**54**	23	23	31	4	28
Poltavaregion	**15**	6	6	9	3	6
Rivne region	**25**	8	8	17	5	13
Sumyregion	**31**	6	6	25	4	21
Ternopilregion	**13**	4	4	9	7	5
Kharkiv region	**34**	5	5	29	7	22
Khersonregion	**17**	5	5	12	2	8
Khmelnitsky region	**10**	2	2	8	0	8
Cherkasyregion	**17**	4	4	13	3	10
Chernivtsi region	**58**	0	0	58	123	8
Chernihivregion	**19**	7	7	12	3	9
Total, by regions	**1 018**	**153**	**153**	**865**	**501**	**420**
Total in Ukraine	**1 018**	**153**	**153**	**865**	**501**	**420**

*without regard to criminal offenses excluded from accounting in connection with the termination of proceedings on the basis of paragraphs 1, 2, 4, 6, of the part 1 of Article 284 of the Code of Criminal Procedure of Ukraine

** taking into account the criminal production of previous years

Note: Registered crimes are defined as per articles 361-363-1 of the Criminal Code of Ukraine) and the results of their pre-trial investigation in the context of the regions of Ukraine.

Source: Cybercrime statistics Ukraine (2018)

It should be noted that the loss of the Ukrainian citizens from the actions of cyber fraudsters in 2016 increased approximately 4 times and amounted to 339,2 million UAH. Most often, organized criminals use the most commonly perpetrated types of fraud, such as wishing calls and crimes on the Internet. Over the year, the level of cybercrime with the use of wishing increased by 5,3 times and amounted to 275,5 million UAH, while the loss of users of payment cards from fraudulent transactions in the Internet increased by 2 times, to 63,7 million UAH (Finance UA 2017).

In the recent years, the largest number of cyber crimes in the world has been diagnosed in the sphere of financial relations between state structures, retail enterprises and consumer goods production enterprises. In particular, in 2016, the sphere of communication and insurance services, the chemical and pharmaceutical industries, state organizations and enterprises suffered most of all from cybercrime.

Thus, in the field of information security there are many problems that can not be fully resolved by traditional means, and which should be brought to the attention of society and public authorities.Large-scale violations involving all aspects of society, which are based on the latest methods of attacking computer networks, as well as management of public consciousness, require a systematic approach to creating an integrated information security system that can withstand these threats. A general analysis of the issues of protection from threats that arise again and again, and continue to evolve, can be referred to as “cybersecurity”. The issues of ensuring cybersecurity were described in a number of scientific papers (PwC 2016; Kavun and Golubev 2013; Kolesnik et al. 2003; Naumov et al. 2018; Marutian 2017; Nevoit 2017; Olshanska 2015; Pusak and Marchenko 2018; PwC 2018), which determined the need to take large-scale measures on the part of the state to ensure security in the field of information technology.However, unlike the consideration of the problems

of ensuring cybersecurity from the position of a technical, programmatic or organizational approach, it is proposed to consider this problem from the position of organizational and legal approach.

3 Methods, results and discussion

The foregoing led to the formulation of the purpose of the paper, which consists of analyzing cyber security, identifying bottlenecks for cybersecurity and identifying areas of its support and ensuring program. At the same time, for the correct formation and solution of the problems of ensuring cybersecurity in public administration systems, as well as management systems of economic entities, it is necessary to continue the efforts: i) to carry out the analysis of cybersecurity of Ukraine as a leading threat to information security; ii) to consider the legal provision of national cybersecurity in the range of information security problems; and iii) to offer conceptual solutions to the problem of ensuring cybersecurity.

Technologies are constantly evolving, and new cyber threats continue to be created. As part of technological progress, cybersecurity must be an integral part of progress itself. Unfortunately, cybersecurity is not yet among the key factors in the national and industrial technology strategy of a large number of the countries. The government of each country should be aware of its current level of competence in the field of cybersecurity. Additionally, it is important to identify those areas where cybersecurity control needs to be strengthened. To this end, a joint project was implemented between ABI Research and the International Telecommunication Union, which resulted in the analysis of the Global Cybersecurity Index of 193 countries in 2015. Furthermore, it allowed assessing the level of participation of independent states in the field of cybersecurity.

Global Cybersecurity Index (2017) is the main achievement of the collective partnership between the private sector, the state and the international organization. It aims to bring the issue of cybersecurity to the priorities of national strategies of different countries (Global Cybersecurity Index and Cybersecurity Profile 2018). The Index is built on the basis of the Global Cybersecurity Agenda, which was launched by the International Telecommunication Union. Moreover, it estimates the level of fulfillment of obligations in the following five spheres: legal measures, technical measures, organizational measures, potential development and international cooperation (ITU Global Cybersecurity Index 2018). For each of these areas, relevant questions for evaluation have been developed. With the help of consultations with the expert group representatives, these questions were weighed, in order to obtain a common index score. Our analysis of the dynamics of the global index of cybersecurity for 2015-2017 has determined that only three out of five countries were able to maintain their leading positions in the rating. There is a growth in the Ukrainian cybersecurity index from 0,353 in 2015 to 0,501 in 2017, that is, the government of the country was able to achieve significant changes in this area and change its position in the rating (from 71 to 59). At the same time, it is not advisable to compare the economic, social and technological, in particular cyber, development of the world's leading countries and Ukraine, as a country with a transformational economy. Therefore, it is proposed to consider the indicators of the Global Cybersecurity Index under conditions equivalent to Ukraine (See Table 2).

Table 2. Rating of the Commonwealth of Independent States (CIS) region based on the 2015 index

Commonwealth of Independent States	Legal measures (2015)	Technicalmeasures (2015)	Organizationalmeasures (2015)	Potential development (2015)	International cooperation (2015)	Index (2015)	Regional Rating(2015)	Index (2015)	Regional Rating(2017)
Azerbaijan	0,7500	0,5000	0,5000	0,5000	0,5000	0,5294	1	0,559	4
Georgia	0,7500	0,6667	0,7500	0,2500	0,2500	0,5000	2	0,819	1
Russian Federation*	1,0000	0,3333	0,5000	0,3750	0,5000	0,5000	2	0,788	2
Moldova*	0,7500	0,5000	0,2500	0,2500	0,3750	0,3824	3	0,418	6
Ukraine*	0,7500	0,3333	0,2500	0,1250	0,5000	0,3529	4	0,501	5
Armenia	0,5000	0,5000	0,0000	0,0000	0,1250	0,1765	5	0,196	11
Belarus*	0,7500	0,3333	0,0000	0,0000	0,1250	0,1765	5	0,592	3
Kazakhstan*	0,7500	0,3333	0,0000	0,0000	0,1250	0,1765	5	0,352	7
Tajikistan*	0,7500	0,0000	0,0000	0,0000	0,2500	0,1471	6	0,292	8
Uzbekistan*	0,7500	0,1667	0,0000	0,0000	0,1250	0,1471	6	0,277	9
Kyrgyzstan*	0,5000	0,0000	0,0000	0,0000	0,2500	0,1176	7	0,270	10
Turkmenistan*	0,7500	0,0000	0,0000	0,0000	0,0000	0,0882	8	0,133	12

*on the basis of secondary data
Source: Own results

In the field of cybersecurity of many post-Soviet countries, including Ukraine, we consider it worthwhile to note such problem areas as:

- the absence of CERT Coordination centers;
- the low level of standardization for organizations;
- child safety in cyberspace;
- lack of incentive mechanism for the industry;
- interagency cooperation (Marutian 2017).

In Ukraine the most problematic indicators of the Index are the following ones: the absence of sectoral cybersecurity centers; the lack or low standards of cybersecurity of organizations and professional standards in this field; Internet safety for children; the practical implementation of activities; incentive mechanisms for the industry; the lack of a national or sectoral roadmap for cybersecurity in Ukraine; the lack of recognized national comparative analysis and reference for measuring cybersecurity; lack of the necessary number of specialists in the public sector, certified internationally.

Analysts of the International Telecommunication Union identified the most significant positive indicators of the cybersecurity in Ukraine, which are the following ones: legislative base, professional education, state regulation of cyber security issues, interagency and international cooperation in this area and the level of public-private partnership.

For completeness of the study, it is proposed to investigate the indicator of the new index of protection of the cyberspace of a certain country, the so-called "National Index of Cybersecurity" (NCSI), which measures the countries' preparedness to prevent the implementation of fundamental cyber threats, as well as the readiness to manage cyber incidents, crimes and large-scale cybercrimes. Ukraine currently occupies the third place in this index, taking into account the positive indicators in general, especially with regard to the country's ability to develop a cybersecurity policy, the ability to fight against cybercrime and to provide electronic identification and electronic signature services (See Figure 1) (NCSI 2018).

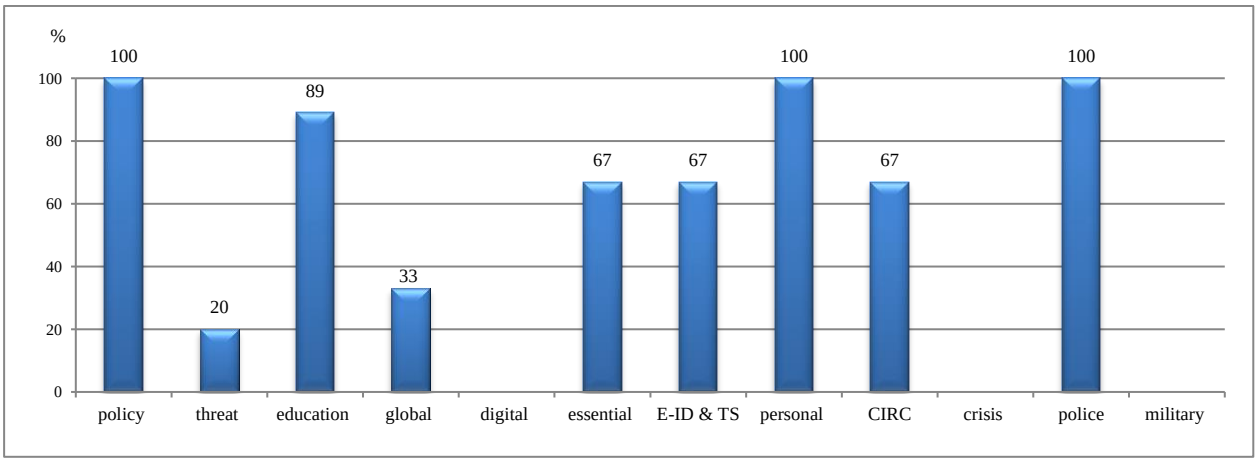

Fig. 1. Components of the National Cybersecurity Index of Ukraine in 2018, %
Source: Own results based on NCSI (2018)

Therefore, in accordance with the National Cybersecurity Index, the main shortcomings in cyber defense in Ukraine are as follows:

- the lack of protection of digital services (the lack of responsibility of providers for digital services providing, the lack of cybersecurity standards for the public sector and the lack of a competent supervisory authority);
- the lack of cyber crisis management (the absence of crisis management planning in the field of cyber crisis management, lack of management activities to prevent cyber crisis at the national level of the examined country, indifference in international anti-crisis management activities in the field of cyber crisis management, the lack of operational support for volunteers in cyber crisis management);
- the absence of military cyber operations (the lack of units for the implementation of cyber operations, indifference in international events to improve military cyber operations, the lack of experience in conducting military cyber operations).

The main advantages of cybersecurity in Ukraine, according to the National Index, are the following ones:

- cybersecurity policy development (creation of a cybersecurity management body – the Department of Cyber Police of the National Police of Ukraine, the existence of a cybersecurity policy coordination format, an effective cybersecurity strategy and a plan for its further implementation);
- existence of an effective system for the protection of personal data (the existence of legislation on the protection of personal data, the existence of a special body for the protection of personal data);
- fight against cybercrime (cybercrimes are recognized as criminalized ones, the presence of actors in the fight against cybercrime, the existence of subjects to combat "digital" crime, round-the-clock support for combating international cybercrime).

It is worth noting that such indicators in the Global Cybersecurity Index and in the National Cybersecurity Index are diametrically opposite in meaning, which can be explained by different approaches and criteria for assessing a certain group of indicators. Summarizing the aforesaid, it is proposed to identify the leading problems of ensuring the proper level of cybersecurity of Ukraine:

- lack of unification of the categorical apparatus in the legislation of the country in the field of cybercrime;
- lack of appropriate specialists in the field of cybersecurity;
- lack of standards of cybersecurity in organizations and professional standards in this field;
- absence of sectoral cybersecurity centers;
- lack of generally accepted national comparative analysis and reference for measuring cybersecurity; the severity of identification, investigation and disclosure of cybercrime.

The need to prevent and combat cybercrime predetermines, first of all, the need for an analysis of its legal and organizational support. The problem of protection against cybercrime in Ukrainian organizations at all levels and forms of ownership is complicated by the lack of appropriate policies and developed mechanisms for responding to cyberattacks. The most common variants of their reaction are: to involve their own experienced specialists to solve the problem; seeking assistance from independent experts; informing law enforcement agencies. As a rule, outside consultants are involved in the occurrence of the incident (this was reported by 57% of the organizations surveyed), and only 21% of organizations in Ukraine address external experts for preventive purposes (PwC 2016).

Until recently, the main legal acts that form the legal framework for combating cybercrime in Ukraine are: Convention on Cybercrime ratified by Ukraine (Conventions on curtailment 2005), the Law of Ukraine "On ratification of the Convention on Cybercrime" (Convention on Cybercrime 2015), the Criminal Code of Ukraine (2001), the Law of Ukraine "On Information Protection in Automated Systems" (Verkhovna Rada of Ukraine 2005). However, the conceptual-categorical apparatus of cybercrime in them is not sufficiently defined and remains uncoordinated: there is no single interpretation of the concept of "cybercrime", and other synonym terms are often used instead.

The use of a large number of synonym terms in this sphere often does not have a proper explanation, therefore different understandings of the essence of the given term are encountered in various regulatory legal acts. For example, in the Law of Ukraine "On the Fundamentals of the National Security of Ukraine" (Verkhovna Rada of Ukraine 2003) and in the Doctrine of Information Security of Ukraine (President of Ukraine 2017) we find just a reference to such concepts as "computer crime" and "computer terrorism", but we do not see a clear definition of their essence. Insufficient clarity of the conceptual apparatus in the field of combating cybercrime does not allow: to objectively assess the crime situation in the national segment of cyberspace; to identify the most effective measures to combat cybercrime; to clearly articulate the tasks and functions of actors in the fight against cybercrime; and to form an effective system of accounting and analysis of information on combating cybercrime. On May 9, 2018, the Law of Ukraine "About the basic principles of ensuring cybersecurity of Ukraine", dated 05.10.2017 No. 2163-VIII (Verkhovna Rada of Ukraine 2017) came into force, which determines, in particular, the legal and organizational basis for ensuring the protection of vital human and citizen interests, society and state, as well as the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cybersecurity. It defines key terms in the field of cybersecurity, in particular cybersecurity, cyberattack, cyberspace, cyber threat, cybercrime (computer crime). Obviously, there is a need to harmonize the relevant provisions of Regulations related to this Law.

4 Conceptual solutions to the problem of ensuring cybersecurity

Proceeding from the Law of Ukraine "On the Ratification of the Convention on Cybercrime", the body entrusted with the authority to establish and operate a 24-hour contact network to provide emergency assistance in the investigation of crimes involving computer systems and data, prosecution of persons accused of such crimes, as well as the collection of evidence in electronic form is the Ministry of Internal Affairs of Ukraine. In December 2011, the Department for Combating Cybercrime of the Ministry of Internal Affairs of Ukraine was established, and the corresponding territorial units started to be created only in early 2012. One of the problems in the work of employees of this structure is the need to own information technology, a deep knowledge of the principles of networks and devices used to commit offenses, and the knowledge of the latest developments in the IT industry. Taking this into account, additional training and continuous professional development of specialists in the cybersecurity sphere are required.

One of the factors contributing to the growth of cybercrime is the lack of appropriate specialists with the necessary competencies. Only in four out of ten organizations, according to sociological research, there are specially trained workers who are ready to respond to incidents in the field of cyberspace (PwC 2016). One of the ways to solve the current situation is to attract specialists from the leading countries of the world in the field of cybersecurity and the formation of the suitable domestic institutions for training specialists of the appropriate level in this area.

Consideration of the existing approaches and "best practices" in ensuring information security of business and the state in Ukraine allows us to conclude that there is already a procedure for certification of protection equipment for acceptable requirements. Moreover, there are not only various tools of ensuring security, created in Ukraine, but also certain "templates" from the most reliable cyber defense systems of the Western countries. However, there is also such a problem as the lack of unified databases and knowledge bases of incidents of information security. Another important task is the creation of sectoral cyber defense centers. Among the main functions of the cybersecurity system should be the next ones: the identification of cyberattacks, data protection, response to cyberattack and the full restoration of the organization.

According to the estimates of the domestic and foreign experts, solving the problems of investigating and uncovering cybercrime is extremely difficult for law enforcement agencies, both in our country and abroad. In particular, today in Ukraine the level of computer crime latency is 90%, and of the remaining 10% of revealed computer crimes, only 1% is disclosed, and even smaller percentage of solved crimes ends with a conviction of a court (Kolesnik et al. 2003). The complexity of disclosing such crimes is determined by the following factors: latency; a rather long period of concealment of the fact of committing a crime; a later appeal to law enforcement agencies; lack of uniform standards in solving this problem; remoteness of the offender from the object of encroachment and the possibility of committing cybercrime from virtually anywhere in the world; the complexity of detecting, fixing, seizing forensic significant information when performing investigative actions for use as evidence; anonymity, non-personal identification of criminals; the irrational nature of cybercriminals.

4 Conclusions

On the basis of the aggregation of indicators of Global Indices, the strengths of cyber security of Ukraine were identified, among them: state regulation of cybersecurity issues, interagency and international cooperation in this field, an appropriate level of public-private partnership, in particular the creation of a cybersecurity policy body, the existence of an effective system for the protection of personal data, the recognition of cybercrime as a criminalized one. Similarly, the leading problems of ensuring the proper level of cyber security in Ukraine have been identified, which are as follows: the lack of adequate specialists in the field of cybersecurity, the lack of unification of the categorical apparatus in the legislation of the country in the field of cybercrime, the lack of cybersecurity standards in organizations and professional standards in this field, the lack of sectoral cybersecurity centers, the absence of a recognized national comparative analysis and reference for measurement cybersecurity, the severity of identification, investigation and disclosure of cybercrime.

Analysis of legal support for national cybersecurity has determined the existence of a significant number of regulatory and legal acts, which mainly indirectly affect the issues of information security and cybersecurity in particular. However, the use of a large number of synonym terms in this sphere often does not have a proper explanation, therefore, different understandings of the essence of the given term are encountered in various regulatory legal acts. Insufficient clarity of the conceptual apparatus in the field of combating cybercrime does not allow: to objectively assess the crime situation in the national segment of cyberspace; to identify the most effective measures to combat cybercrime; to clearly articulate the tasks and functions of actors in the fight against cybercrime; and, finally to form an effective system of accounting and analysis of information on combating cybercrime. Obviously, there is a need to harmonize the relevant provisions of Regulations that are related to this Law.

In order to overcome certain shortcomings, the conceptual ways of solving the problem of ensuring cybersecurity have been proposed and characterized, which mainly consist in improving the legal and organizational support for the information and cyber security of Ukraine. These ways are related to the legal regulation of the information security and cyber security, the involvement of specialists from the leading countries of the world in the field of cybersecurity and the formation of the domestic institutions for training specialists of the appropriate level in this area, the formation of unified databases and knowledge bases of incidents of information security, the creation of sectoral cybersecurity centers.

According to the established hypothesis, it is determined that the effectiveness of the fight against cybercrime in Ukraine primarily depends on improving its legal and organizational support. And in this context, it is important to use a single conceptual-categorical apparatus of cybercrime in all normative and legal acts, to improve the skills and appropriate training of law enforcement agencies that deal with the disclosure of computer crimes, the establishment of sectoral cyber defense centers, and the strengthening of international cooperation in the field of preventing and investigating cybercrime. Therefore, a promising direction of the study is the detailed development of the program of actions necessary to form an additive mechanism of information security and cyber defense of the domestic information space.

References

Bychkova S, Makarova N, Zhidkova E (2018) Measurement of information in the subsystem of internal control of the controlling system of organizations of the agro-industrial complex. Entrepreneurship and Sustainability Issues 6(1):35-43. doi: 10.9770/jesi.2018.6.1(3)

Čábelková I, Abrhám J, Strielkowski W (2015) Factors influencing job satisfaction in post-transition economies: the case of the Czech Republic. International Journal of Occupational Safety and Ergonomics 21(4):448-456. doi: 10.1080/10803548.2015.1073007

Convention on Cybercrime (2015) On Ratification of the Convention on Cybercrime: The Law of Ukraine. http://zakon2.rada.gov.ua/laws/show/2824-15 Accessed 26 Jul 2018

Conventions on curtailment (2005) Ratified by cautions and declarations by Law No. 2824-II dated 07 November 2005. Official site of the Supreme Rada of Ukraine. http://zakon5.rada.gov.ua/laws/show/994_575 Accessed 28 Jul 2018

Criminal Code of Ukraine (2001). Criminal Code of April 5. 2001 № 2341-III. Official site of the Verkhovna Rada of Ukraine. http://zakon4.rada.gov.ua/laws/show/2341-14 Accessed 20 Jul 2018

Cybercrime statistics Ukraine (2018) Request to the General Prosecutor's Office of Ukraine. https://dostup.pravda.com.ua/request/statistics_kibierzlochinnosti_v Accessed 19 Aug 2018

Finance UA (2017) Cybercrime is not sleeping – how not to get into the net of scam artists. https://news.finance.ua/ru/news/-/395023/kiberzlochynnist-ne-spyt-yak-ne-potrapyty-v-siti-aferystiv Accessed 28 Aug 2018

Global Cybersecurity Index (2017) http://j-times.ru/rejting/globalnyj-indeks-kiberbezopasnosti-2017.html Accessed 21 Jul 2019

Global Cybersecurity Index and Cybersecurity Profile (2018) Report. ABI Research. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-R.pdf Accessed 27 Jul 2018

ITU Global Cybersecurity Index (2018) https://digital.report/globalnyiy-indeks-kiberbezopasnosti-ot-itu-gruziya-i-rossiya-voshli-v-top-10/#prettyPhoto Accessed 27 Jul 2018

Kavun SV, Golubev VO (2013) An Analysis of Cybercrime in the Sphere of Economic Security.Scientific Papers "The Black Sea State University named after Petro Mohyla of the Kyiv-Mohyla Academy Complex". Computer Technology 229(217): 9-13.

Kolesnik VL, Gora IV, Kosin MI, *Investigation of computer crimes: scientific methodical manual*, 1st edn. (Kyiv, Publishing House of the National Academy of the Security Service of Ukraine, 2003), 124 p.

Lisin E, Rogalev A, Strielkowski W, Komarov I (2015) Sustainable modernization of the Russian power utilities industry. Sustainability 7(9):11378-11400. doi: 10.3390/su70911378

Markina I (2016) Administrative-legal mechanism of economic security system of the country. Actual Problems of Economics 9: 69-77.

Marutian R (2017) Ukraine took 56th place in the global index of cyber security. MATRIX. http://matrix-info.com/2017/06/28/ukrayina-posila-56-mistse-u-globalnomu-index-kiberb ezpeky/ Accessed 20 Jul 2018

MBC (2018). Statistics. http://mvs.gov.ua Accessed 17 Jul 2018

Moyseyenko I, Ryvak N (2016) Indirect taxes in the mechanism of state regulation. International Economics Letters 5(2):63-71. doi: 10.24984/iel.2016.5.2.4

Naumov O, Gryshova I, Rozsa Z (2018) Leadership in Energy efficiency of agro-industrial production: regional Aspects. In: Strielkowski W, Chigisheva O (eds.) Leadership for the Future Sustainable Development of Business and Education. Springer Proceedings in Business and Economics. Springer, Cham, pp. 579-590. doi: 10.1007/978-3-319-74216-8_58

NCSI (2018) National Cyber Security Index. https://ncsi.ega.ee/country/ua/?pdfReport=1 Accessed 29 Jul 2018

Nevoit YaV (2017) Analysis of threats of information security in the period 2015-2016.Modern security of information 2(30):79-84.

Oláh J, Bai A, Karmazin Gy, Balogh P, Popp J (2017) The Role Played by Trust and Its Effect on the Competiveness of Logistics Service Providers in Hungary. Sustainability 9(12):2303. doi:10.3390/su9122303

Olshanska OV (2015) The main provisions of information security and its state in modern conditions of development in Ukraine. History KNUTD, Series "Economic sciences 2(85):62-68.

President of Ukraine (2017) The doctrine of information security of Ukraine: put into effect by Decree of the President of Ukraine dated February 25, 2017, 47/2017. http://www.president.gov.ua/documents/472017-21374 Accessed 28 Jul 2018

Pusak YYa, Marchenko OM (2018) Problematic aspects of prevention and counteraction of cybercrime in Ukraine. Materials of the International scientific and practical conference "Economic and informational safety: problems and prospects", Dnipro: Dniprovsky State University of Internal Affairs, pp. 173-176.

PwC (2016) World Economic Crime Survey for 2016. https://www.pwc.by/en/publications/other-publications/economic-crime-survey-2016.html Accessed 27 Aug 2018

PwC (2018) Ukraine. World Economic Crime Review. Cybercriminals are at the center of attention. https://www.pwc.com/ua/uk/press-room.assets/GECS_Ukraine_en.pdf Accessed 27 Jul 2018

Shvetsova OA, Rodionova EA, Epstein MZ (2018) Evaluation of investment projects under uncertainty: multi-criteria approach using interval data. Entrepreneurship and Sustainability Issues 5(4): 914-928. doi:10.9770/jesi.2018.5.4(15)

Verkhovna Rada of Ukraine (2003) On the Fundamentals of National Security of Ukraine: Law of Ukraine. Bulletin of the Verkhovna Rada of Ukraine (VVR), 39, Art. 351. http://zakon2.rada.gov.ua/laws/show /964-15 Accessed 28 Jul 2018

Verkhovna Rada of Ukraine (2005) On Amendments to the Law of Ukraine "On Information Protection in Automated Systems": Law of Ukraine, Bulletin of the Verkhovna Rada of Ukraine (VVR), 26, Art. 347. http://zakon3.rada.gov.ua/laws/show/2594-15 Accessed 28 Jul 2018

Verkhovna Rada of Ukraine (2017) On the Basic Principles of Cybersecurity Protection of Ukraine: Law of Ukraine. Bulletin of the Verkhovna Rada (VVR), 2017, 45, Art.403. http://zakon5.rada.gov.ua/laws/show/2163-19. Accessed 28 Jul 2018

Zielińska A (2016) Information is a market products and information markets. Czech Journal of Social Sciences, Business and Economics 5(4):31-38. doi: 10.24984/cjssbe.2016.5.4.4