THE MAIN DIRECTION OF CYBERCRIME PREVENTION IN UKRAINE

Khrystyna VOROBETS

Covered in:
CEEOL, Ideas RePeC, EconPapers, Socionet, HeinOnline

Published by:
Lumen Publishing House
On behalf of:

STEFAN CEL MARE UNIVERSITY FROM SUCEAVA,
FACULTY OF LAW AND ADMINISTRATIVE SCIENCES,
DEPARTMENT OF LAW AND ADMINISTRATIVE SCIENCES
THE MAIN DIRECTIONS OF CYBERCRIME PREVENTION IN UKRAINE

Khrystyna VOROBETS 1

Abstract
The rapid growth of information and communication technologies determined the occurrence of new hardware, software components and other applications, which were exploited in a form of other by criminal organizations. The way in which offenders in cyberspace exploit the new technologies is really remarkable.

The number of different cyber operations including cyber attacks are rising. Cyber threats represents serious risks to both public and private sectors, endangering cyber security of individual states and international security as a whole. Cyber attacks consists of various actions disrupting, denying or destroying computers and computers networks. In the author’s view any activity in cyber space must comply with the rules of international law. This article explores the varying conceptualisations of cybercrime before identifying tensions in the production of criminological knowledge that are causing the rhetoric to be confused with reality. Also analyzes the main directions of crime prevention in Ukraine.

Considering the issue of counteracting cybercrime, it is advisable to join those criminologists who distinguish the general social, special-criminological and individual ways of counteraction. The cybercrime at the general social level (direction) includes a set of promising socio-economic, organizational, administrative, ideological, cultural and educational and other measures aimed at solving urgent social problems and contradictions in the country. It is the realization of general social measures of prevention that allows to eliminate or minimize the influence of criminogenic determinants of cybercrime, to prevent the formation of an offender’s personality.

Keywords:
Cybercrime, informatization; communication technologies; information security; cyber attacks.

1 PhD student of the Department of public law, Faculty of Law, Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine, e-mail: k.vorobets@chnu.edu.ua, phone: +380660923743
I.1. Definition of the concept of Cybercrime

Access to the Internet and electronic social media have become essential for the effective exchange of diverse opinions important for the practical realization of the freedom of expression. If universal Internet access is to be recognized internationally as a universal right, a derivative of the right to freedom of expression, perhaps, it is the right time to entertain the idea of an international framework convention to guarantee a minimal standard of practices acceptable for the exchange of information and opinions on the Internet [8: 189].

One of the main priorities of Ukraine is the desire to build a people-centered, legal and informational society open to all. The main strategic goal of the development of such a society is to accelerate the development and implementation of the latest competitive information technology in all spheres of public life.

Today, cybercrime is one of the most dynamic groups of socially dangerous attacks. The rates of spread of these crimes are rapidly increasing, and their social danger is constantly increasing. This is due to the accelerated development of science and technology in the field of computerization, as well as the constant and rapid expansion of the scope of computer technology.

Distribution of computer viruses, plastic card fraud, theft of funds from bank accounts, the theft of computer information and violation of the rules of operation of automated electronic computing systems - this is far from a complete list of similar crimes. This category of crimes is called differently: cybercrime, computer crimes, crimes in the field of computer technology, crimes in the field of computer information.

The specificity of this type of crime lies in the fact that the preparation and commission of a crime is carried out, practically, without leaving the "workplace". Since computer technology is constantly getting cheaper, crimes can be committed from anywhere in the world, in any locality, and objects of criminal assault can be thousands of miles away from the perpetrator. In addition, it is rather difficult to detect, fix, and remove forensic-meaningful information when conducting investigative actions to use it as evidence. All this, of course, is an advantage for cybercriminals [10].

In modern conditions, for the most part, most social processes are transferred to the virtual space. This process is an integral part of the development of the information society and the basis of the formation of the information economy.
According to most experts, the information economy is an economic relationship in which the emphasis is on the leading role of electronic information technology in the development of all major spheres of the economy. Information itself is identified with commodity products and is mainly investigated by statistical methods. That is why, in an era of unceasing development of information technology, computer networks and the Internet, cybercrime has become a reality of social life.

Unlike print media or broadcasting, the Internet remains almost unregulated. Anyone who has a personal computer or smartphone can access practically any source of information on the Internet. The growing share of business operations (for example, the sale of various goods and services) and public services (for example, filing tax returns) goes to the Internet, which leads to an increase in the number of losses caused by cybercrime. A good example of this issue was the Wannacry, from which private and public organizations in 150 countries became victims of an unprecedented scale.

Some countries, such as China, have recognized the potential impact of the Internet on public opinion and have tightly controlled the content of freedom of speech. While Western democracies are struggling with the dilemma of cybercrime, while keeping web electronic media open for a fair exchange of thoughts and information. So what is the ultimate goal of a social e-platform that acts as a freedom of speech: making a profit, moving a certain point of view, or maybe pursuing some other goal? [8: 185].

One of the key benefits of the Internet lies in the fact that it is mostly free. Even a critically-minded user can now find the most varied point of view on the Internet on one or another issue, as Mark Zuckerberg pointed out in his statement. At the same time, it is obvious that electronic platforms of electronic media should be responsible for spreading "socially dangerous" false news. And if so, who decides what information can be freely distributed, and which should be limited? What is the mechanism for regulating such spread?

One of the mechanisms of limiting the impact of fake news was the mechanism of "controversial labels" proposed by Facebook. However, it has been found that this mechanism is practically ineffective. In 2017, a new global survey was conducted in 18 countries of the BBC World Service, which showed that 79% of users worried about fake news on the Internet, while 45% admit false news as a major issue. Another poll conducted by GlobeScan in January-April 2017 revealed that, despite concerns about counterfeit Internet content, an increasing share of Internet users opposes government regulation. On average, in 15 countries, the proportion of those who agree that the Internet should not be regulated by any level of
government has increased from 51% in 2010 to 58% in 2017. Greece (84%),
Nigeria (82%), Brazil (72%), France (71%), Turkey and Kenya (every 70%)
are against any type of state regulation of the Internet. In a number of
Western countries, except Greece and France, the attitude to Internet
regulation is quite mixed. The idea of this in Canada, Australia, Spain and
Germany tends to favor government intervention. In the UK, a narrow but
stable majority (53%) continues to promote certain regulation [3: .71].

Since traditional mass media have almost completely switched to the
Internet and have become a subset of electronic social media, Internet
access is becoming a universal service, similar to access to clean drinking
water. The quality of water is constantly monitored and provided by the
government and taken as a matter of convenience to the general public. If
universal access to the Internet is recognized internationally as a universal
right, derived from the right to freedom of expression, it may be time to
entertain the idea of an international framework convention that would
guarantee a minimum standard of practice that is acceptable for the
exchange of information and ideas on the Internet. This framework
convention does not necessarily have to be compulsory, but at least it would
be the beginning of productive dialogue to more effectively deal with "fake
news" and various types of international cybercrime [6].

To commit a crime, cybercriminals come up with more intricate
schemes every day. From the simplest tricks of the values of a person when
he voluntarily transfers funds to intruders, to theft of the base salary
accounts of employees of the company or institution for further resale, or
penetration into the computer network and the dismantling of industrial
objects. Writing and distributing virus and trojan programs that get on their
computer or phone start to monitor their owner, collect and transmit
information about it and lead to dangerous consequences. Anyone can
become the subject of a crime, even without knowing it.

According to a study by Microsoft Ukraine on the level of computer
security in Ukraine conducted in 2016 in Kyiv, 92% of Ukrainians are not
well-informed about cyber threats. In most Ukrainians, it's easy to forge a
password from mail or to give access to their own information in a social
network, and only 8% understand how to protect themselves from such
cyber threats as phishing, identity theft, etc [8: 184].

It is social engineering today that becomes the main source of
network threats. Only 30% of respondents take care of their reputation on
the Internet, a third of users who have children almost don’t know about
threats online. Also, vulnerable users of cybercrime are over 49 years old -
are not doing anything to protect themselves from cyber threats. According
to the system of monitoring and rapid response to computer threats
Kaspersky Security Network in March this year, on average, over the day, there were recorded more than 800 thousand actions of the system for protecting children from unwanted content on the Internet.

Also, let's draw attention to one of the negative aspects of the development of legal regulation of the fight against cybercrime in Ukraine, as pointed out by O. Wiener, namely: increasing the level of control over the users of the Internet. An example is the recent situation. On June 27, 2017, Ukraine experienced massive cyberattacks by affecting computer systems unknown at the time of the virus. As a result, the virus "Petya.A", or "mbr locker 256", caused a violation of the work of Ukrainian state-owned enterprises, institutions, banks, media, etc. Negative influence was made even on web resources of Cyberpolice and Special Communication Service of Ukraine, which is a significant problem, because these bodies are subjects of the fight against cyber crime in our country. The attack demonstrated the disadvantages and vulnerabilities of the national legal regulation of the mentioned problem, as well as the absence in the national science and practice of the answers to the questions: what are the elements of the mechanism? In particular, as a result, it is quite probable that the measures to increase the efficiency of the special services by means of the normative and actual reduction of the rights and freedoms that are granted to Ukrainian citizens are likely to be strengthened. On the basis of the above main perspective, we see the elimination of borders between states in matters of combating cybercrime [7].

Cybercrime is an international problem, since cyberspace, as an object of its encroachment, is not limited to state borders. That is why the maximum number of countries should be involved in counteracting these negative phenomena, irrespective of geographical location, level of socio-economic and technical development, as well as the level of the adopted national legislation, since a cyber crime can geographically remain and commit crimes even in the most remote corner of the world. That is why technologically advanced states should be able to assist less developed in the prevention and investigation of cybercrime. International law provides a number of grounds for determining territorial jurisdiction or the principle of citizenship.

Most of them are enshrined in international normative legal acts on the prevention of cybercrime. At the same time there are norms that give the subjects of international law certain freedom in such legal relations. For example, the Cybercrime Convention contains a provision that empowers participants to access publicly available computer data stored without permission from the other party, regardless of where they are placed geographically; to access or receive, through a computer system located in its
territory, computer data that is stored and contained in the other party, if the party obtains the lawful and voluntary consent of the person who has the legal authority to disclose them to such party by means of such computer system.

The concept of "cybercrime" first appeared in the US, and then in other foreign literature in the early 1960's and was defined as a violation of other rights and interests in relation to automated data processing systems. At the global level in 2000, the United Nations adopted the United Nations Convention against Transnational Organized Crime in 2000. In accordance with Part 2 of Art. 3 of this Convention, a transnational crime is a crime if: a) it is committed in more than one state; b) it is committed in one state, but a substantial part of its preparation, planning, guidance or control takes place in another state; (c) It is committed in the same State but with the participation of an organized criminal group that engages in criminal activities in more than one State; or (d) it is committed in one state, but its substantive effects take place in another state. The Convention notes that they are to be recognized as transnational crimes in the context of their transboundary committal: participation in an organized criminal group (Article 5), money laundering from crime, including complicity (Article 6), corruption, including complicity (art. 8), provided that they are recognized as transnational [7: 51].

The International Criminal Law on the Provision of IP Development also belongs to the International Covenant on Combating the Financing of Terrorism in 2000. This act states that any person commits an offense if: in any manner, directly or indirectly, illegally and intentionally provides funds or performs their collection with the intention that they are used, or in the knowledge that they will be used, in whole or in part, for the commission of: 1) any act that constitutes a crime under the scope of one of the treaties listed in the annex and to the definition contained therein; 2) any other act aimed at causing the death of any civilian, or any other person who does not actively participate in military operations in a situation of armed conflict, or to cause serious bodily harm, when the purpose of such an act the act, by virtue of its nature or context, is to intimidate the population or force a government or an international organization to commit or abstain from any act (Article 1, Article 2); 3) attempts to commit any of the crimes specified in clause 1 (Article 4, Article 3). A) participates as an accomplice in the commission of any of the crimes specified in paragraph 1 or 4 of this article; 4) organizes or directs other persons for the purpose of committing any of the crimes specified in clauses. 1 or 2. (Clauses 1 and 4 of Article 2 of the Convention); 5) contributes to the commission of one or more of the crimes specified in clauses. 1 or 2. (Articles 1 and 4, Article 2 of the Convention), a
THE MAIN DIRECTION OF CYBERCRIME PREVENTION IN …

group of persons acting for a common purpose. Such assistance should be intentional and should be provided: (a) either for the purpose of supporting the criminal activity or the criminal ends of the group, where such activity or purpose involves committing one of the offenses referred to in paragraph 1 of this article; b) or with the knowledge of the intention of the group to commit one of the crimes specified in paragraph 1 (paragraph 1 of Article 2 of the Convention) (Article 5, paragraph 2). This act is not directly emphasized, but in the context of the development of IP, the prediction of the financing of terrorism and the promotion of such financing, made using remote communication based on ICT, are fully relevant. Therefore, the promotion and direct financing of terrorism and the legalization of proceeds from criminal activity using remote telecommunications, which poses an increased risk due to greater opportunities and less vulnerability of accomplices, should be criminalized. Obviously, the Convention against Transnational Organized Crime and the International Convention for the Suppression of the Financing of Terrorism were adopted by the United Nations at the time of the recognition of the existence of the IP [3:195].

However, the text of these conventions does not indicate a direct opportunity to commit the crimes described in the criminalization of using ICT. However, logically, since the crimes described in them can not physically be prepared and committed without the use of ICTs, it is clear that such use is accepted by the international community a priori. Until this time, at the UN level, an act has not been approved to regulate the requirements for criminalization of actions taken with the use of remote communications, computer systems, other ICTs, or the focus on the need for countries of the world to foresee the criminalization of such a method in domestic law. Obviously, this position of the UN is due to the fact that the development of ICT and the possibility of implementing remote communication, built on it in the world has become too traditional and does not require a separate allocation. In addition, the criminalization of ICT-related crimes (to a certain extent) was endorsed by the 2001 Cybercrime Convention, which was initially open for accession to all countries of the world.

Thus, on November 23, 2001, the Council of Europe Convention on Cybercrime (hereinafter - the Convention) was signed in Budapest to counteract computer crimes and to co-operate and coordinate the activities of law enforcement agencies of different countries. To date, it has been ratified by 18 countries and signed by 25 countries [1]. Ukraine ratified the Convention on September 7, 2005. Subsequently, in July 2006, the pre-dated Protocol to the Convention, ratifying the criminalization of racist and
xenophobic acts committed through computer systems (hereinafter referred to as the "Additional Protocol"), was ratified [9].

It should be noted that the Convention only provides for the definition of concepts such as "national security", "national interests", "threats to national security", "military organization of the state" and "law enforcement agencies", provides a list of acts for which nationally proposed to establish criminal liability and their conditional classification is given. The Convention includes 4 groups of acts, namely: 1) offenses against the confidentiality, integrity and availability of computer data and systems: - illegal access - deliberate access to the entire computer system or a part thereof without the right to do so in order to obtain computer data or with any other unfair purpose; - interference with data, intentional damage, destruction, degradation, alteration or concealment of computer information without the right to do so; - interference with the system - deliberately serious impediment to the functioning of the computer system by the introduction, transmission, damage, destruction, degradation, replacement or incorporation of computer data without the right to do so; - Abuse of equipment, namely the manufacture, sale, purchase, use, distribution or provision for use in other ways; 2) computer-related offenses, including forgery and fraud committed with the use of computers; 3) offenses related to the content of information, in particular child pornography, racism and xenophobia; 4) offenses related to the violation of copyright and related rights, such as the illegal reproduction and use of computer programs, audio / video and other types of digital imprinting, as well as databases and books.

By contrast, already in 2003, the adoption of the Additional Protocol to the Council of Europe Convention on Cybercrime, concerning the criminalization of racist and xenophobic acts committed through computer systems (hereinafter referred to as the "Additional Protocol to the Convention on Cybercrime"), which the Parties to the Convention urged criminalization of four more types of cyber crime. It is obvious that during the time elapsed since the determination of the necessity to unify the legislation in the field of cyber crime criminality in 1990 and the adoption of the cybercrime Convention in 2001 was overlooked, however, during this time, the obvious directions of targeting interests of cybercrime all species. The norms of the Convention on cybercrime were intended not only to identify the types of cyber crime and the nature of counteracting such, but also provided a real opportunity for borrowing and / or implementation of the model laws of the participating countries on the definitions of groups and certain types of cyber crime. In 2003, the Council of Europe adopted the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of racist and xenophobic acts committed through computer
systems. Particular attention in these documents attracts a list of violations that are mandatory for legal limitation in the domestic legislation of the participating countries, as well as a list of violations regarding the inclusion in the domestic law of the member countries of which the Council of Europe makes recommendations. In accordance with the provisions of article one of the first convention, cyber crime is divided into: 1) Offenses against the confidentiality, integrity and availability of computer data and systems: "Illegal access" (Article 2); "Illegal interception" (Article 3); "Intervention in data" (Article 4); "Intervention in the system" (Article 5); "Abuse of devices" (Article 6); 2) Offenses related to computers: "Computer-related fake" (Article 7); "Fraud related to computers" (Article 8); 3) Offenses related to the content, namely - "Offenses related to child pornography" (Article 9); 4) Offenses related to violation of copyright and related rights (Article 10). The Additional Protocol provides a list of crimes related to the criminalization of acts of racist and xenophobic violence committed through computer systems that need to be included in domestic law: 1) "The spread of racist and xenophobic material through computer systems" (Article 3); 2) "The threat from racist or xenophobic motives" (Article 4); 3) "An image of racist or xenophobic motives" (Article 5); 4) "Denial, significant minimization, approval or justification of genocide or crimes against humanity" (Article 6) [4].

It should be noted that the Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime regulate not only the kind or type of crime, according to the object of the crime, but also clearly define the essence of the objective side of the crime. The Resolution of the Council of Europe «How to prevent cybercrime against public institutions in the member states and observer states of the Council of Europe?» No. 1565 (2007) emphasized that all countries are threatened with the use of computer technologies against them for criminal purposes, which prompts immediate concentration efforts to jointly develop an effective system of international protection and response measures. The resolution emphasizes that the implementation of the Convention on Cybercrime by all interested States and the accession of non-member countries to the Council of Europe is one of the important international instruments for resolving this problem.

I.2. Directions of Cybercrime Prevention in Ukraine

Cyberspace is a global area in the information environment. As for the definition of the concept of cybercrime, finding a unique definition is
very difficult, since the problem of definition is the starting point for any attempt to unify the concept. Y. Zaichuk notes that when trying to identify crimes committed in cyberspace, it is important to take into account the spatial and temporal dimensions of crime: in order for a crime to be committed in an offline environment, it must be recognized as a crime that is within the limits of time and space.

New technologies allow violators to commit cybercrime at a much shorter time than in an autonomous space. For example, an illegal transaction can take place at a very long distance within a few milliseconds, or a person can be persecuted in real time. The transition to standardizing the definition of cybercrime is difficult, in the absence of an agreement on basic terminology. Various attempts were made to develop a standard language, to describe various aspects of the concept of cybercrime. Even if the standard definition of cybercrime was not obtained, however, there are a number of functional definitions of this phenomenon.

I would also like to point out that in the national legislation before the adoption of the Law "On the Basic Principles of Cybersecurity in Ukraine" there was no legislative definition of the concepts with the prefix cybercrime: "cybercrime", "cybercrime", "cybersecurity", "cyberspace", "cyber threat", "Cyberattack", "cybernetic protection". On the contrary, there was only the concept of crimes, which are learned using computers, computer systems and electronic communication networks, which are enshrined in Section XVI of the Criminal Code of Ukraine. However, in the Convention itself and the Additional Protocol, it also does not contain the definition of the concept of "cybercrime" and related concepts, but only provides a list of acts for which the national level is proposed to establish criminal liability and their conditional classification.

In the Decree of the President of Ukraine "On the Concept of the Development of the Sector of Security and Defense of Ukraine" of March 14, 2016, the term "cybercrime", "cybercrime", "cyber-threat", "cybersecurity", "Cyber-espionage" and others, but no definition of any of these concepts is also given.

However, the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" in 2017 defined the legal and organizational foundations for ensuring the protection of the vital interests of citizen, society and state, the national interests of Ukraine in cyberspace, the main goals, directions and principles of state policy in the field of cyber security, powers state bodies, enterprises, institutions, organizations, individuals and citizens in this area, the main principles of coordination of their work on the provision of cyber security. In the law, the term "cybercrime" ("computer
THE MAIN DIRECTION OF CYBERCRIME PREVENTION IN …

"cybercrime"") is interpreted as a socially dangerous offense in cyberspace and/or its use, the liability for which is provided for by the law of Ukraine on criminal liability and/or recognized as a crime by international treaties of Ukraine, and cybercrime defined as a set of cybercrime.

There are questions: in which way should counteract computer and other crime in this area? Are there certain achievements in this way and so on? Certainly there are, but unfortunately, according to our convictions, they are somewhat untimely and unsystematic. At the same time, we note that in accordance with the Action Plan for 2018 on the implementation of the Cybersecurity Strategy of Ukraine, approved by the Cabinet of Ministers of Ukraine from July 11, 2018, No. 481-p, the following tasks will be implemented [2]:

1. Preparation of proposals regarding legislative regulation of issues concerning: delineation of criminal liability for crimes in the field of the use of computers (computers), systems and computer networks and telecommunication networks; raising the level of responsibility of officials of state bodies, institutions and organizations for violating the requirements for informing in the established order about unauthorized actions (cyberattacks) in relation to state information resources; the definition of the State Service of Communications of Ukraine responsible for the maintenance of backups of information and information of state electronic information resources; establishment of the mandatory agreement with him of the tasks (projects) of the National Program of Informatization, projects (tasks) for the creation and development of information and telecommunication systems of state bodies, enterprises, institutions and organizations of the state form of ownership.

2. Resolving the issue of: Prohibition of state agencies, enterprises, institutions and organizations of state ownership, except for foreign diplomatic institutions of Ukraine, to procure services (to enter into contracts) on Internet access from telecommunications operators (providers), in which there are no documents confirming the conformity of the system protection of information in the area of information protection; introduction of mandatory requirements for the implementation of state-owned bodies, enterprises, institutions and organizations of state ownership of the identification and authentication of the sources of received updates to the software used to process the state information resources and information the protection requirement of which is established by law and to establish the integrity of such updates. ; application by official (official) persons of state bodies, enterprises, institutions and organizations of the state form of electronic digital signature during the use of e-mail for performance of official (official) duties; determination of the procedure for
transferring, storing and accessing backups of information and information of state electronic information resources for the needs of state bodies, especially the subjects of the security and defense sector, financial, energy and transport sectors; formation of a list of objects of critical information infrastructure; determination of the procedure for forming and ensuring the functioning of their state register; Determination of the requirements for an independent audit of information security on critical infrastructure objects.

3. Improvement of interaction between actors providing cyber security through: creation of a single interactive database of cybercriminals for the needs of the Ministry of Defense, SSSU, SBU, National Police, National Bank, intelligence agencies; organizing the exchange of information on cyber attacks on critical infrastructure objects (primarily energy, transport, banks).

4. Reconciliation of the projects (tasks) of the National Program of Informatization, implementation of which is foreseen in 2018, with the Administration of the State Special Communication Service and the State Agency for E-Governance.

5. Improvement of the legal framework by: further implementation of the norms of international standards, EU and NATO standards in the field of electronic communications, information security, information security and cyber security; implementation of Directive (EC) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to improve the overall level of safety of networks and information systems in the EU.

6. Development of a mechanism for attracting individuals and legal entities to fulfill the tasks of cyber defense of state electronic information resources in the framework of public-private partnership on the conditions of outsourcing.

7. Development of the National Telecommunication Network, regulation of the issues of the order of providing services and their tariffing.

8. Conduct modernization of situational centers on cybersecurity of the SSSU and the SBU by attracting NATO assistance in the framework of the implementation of the Cybersecurity Ukraine-NATO Trust Fund.

9. Ensuring the development of the organizational and technical model of cyber defense, in particular the establishment of a center for responding to cyber threats, as well as the development of a system of secure access of state authorities to the Internet.

10. Working out the issue of creating a training cybercenter in the interests of the subjects of providing cyber security.

11. Improvement of the mechanism of interaction with the National Academy of Sciences and its specialized institutions for the purpose of
carrying out scientific research and joint scientific and practical works in the areas of cybersecurity and cyber defense of critical infrastructure.

12. Ensuring the activities of the National Bank's Cyber Defense Center, improving the cyber security and cyber security of the Ukrainian banking system and in the area of money transfer.

13. Development of a methodology for the formation and definition of key indicators of the effectiveness of the Strategy of Ukraine's cybersecurity, taking into account the experience of European and world practices.

14. Participation in measures to strengthen international cooperation by establishing joint bilateral or multilateral groups to carry out cybercrime investigations, as well as joint operations, exchange of information and experience.

15. Organization and holding of conferences, seminars, forums, round tables, training, cybersecurity and cyber-security exercises at the national and international levels.

16. Development of training system in the field of cybersecurity, in particular: training of tactical and operational-tactical level specialists in the direction of "Cyber Security"; preparation, certification, re-certification and advanced training of specialists in the field of cyber defense for the needs of state bodies, military formations and law enforcement agencies.

17. Designing a secure data center (data center) for the needs of government agencies, especially security and defense sector, financial, energy and transport sectors.

18. Implementation of measures for the establishment of the National Center for Operations and Technical Management of Telecommunication Networks of Ukraine.

We believe that for the comprehensive fight against cybercrime to strengthen the economic foundations of the functioning of the security of enterprises, institutions and organizations, the above-mentioned measures should be intensified. Taking into account the transboundary nature of cybercrime, the cooperation of law enforcement agencies in the investigation of cybercrime needs to be operational at the operational level; creation and maintenance of functioning of the mechanism for solving jurisdictional issues in cyberspace. In today's information society, where cyber threats are widespread and will continue to spread, it is important to constantly and systematically and in a timely manner take effective measures to combat cybercrime, as well as to improve its methods and forms of prevention. This applies to virtually all spheres of social and public life, entrepreneurial and socio-humanitarian environment.
REFERENCES


