4. КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ. КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО. КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА. СУДОВА ЕКСПЕРТИЗА. ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ. СУДОУСТРІЙ. ПРОКУРАТУРА ТА АДВОКАТУРА.

УДК 343.3

Oksana Vivchar,
Doctor of Philosophy, assistant professor,
the Faculty of the Financial and Economic
Security an Intellectual Property
Ternopil National University of Economics

CONTEMPORARY PRAGMATICS AND VECTORS OF COMBATING CYBERCRIME IN THE CONTEXT OF INFORMATION AND ECONOMIC SECURITY STRENGTHENING

Key problem aspects of combating cybercrime activity in modern globalization conditions have been considered. In the process of study the main indicators of cybercrime analysis and identification of tasks diagnostic in the field of information technologies have been grounded. Based on this information the ways of combating cybercrime in the context of strengthening information and economic security have been proposed.

Keywords*:cybercrime, cybercrime activity, information and economic security, combating cybercrime.*

Вівчар О.

Сучасна прагматика та вектори протидії кіберзлочинів в контексті зміцнення інформаційно-економічної безпеки

Розглянуто ключові проблемні аспекти протидії кіберзлочинній діяльності в сучасних глобалізаційних умовах. В процесі дослідження обґрунтовано основні показники щодо аналізування кіберзлочинності та ідентифікацію діагностики завдань в сфері інформаційних технологій, на основі чого запропоновано способи протидії кіберзлочинності в контексті зміцнення інформаційно-економічної безпеки.

Ключові слова: *кіберзлочин, кіберзлочинна діяльність, інформаційно-економічна безпека, протидія кіберзлочинам.*

Вивчар О.

Современная прагматика и векторы противодействия киберпреступности в контексте укрепления информационно-экономической безопасности

Рассмотрены ключевые проблемные аспекты противодействия киберпреступных деятельности в современных глобализационных условиях. В процессе исследования обоснованы основные показатели по анализу киберпреступности и идентификацию диагностики задач в сфере информационных технологий, на основе чего предложены способы противодействия киберпреступности в контексте укрепления информационно-экономической безопасности.

Ключевые слова: *киберпреступность, киберпреступная деятельность, информационно-экономическая безопасность, противодействие киберпреступности.*

A problem statement and its relevance. In modern transformational conditions information and economic security of the country depends more on technical infrastructure and its protection. It should be noted that cybercrime always accompanied governmental activity. In such circumstances, to improve the fight against cybercrime, Ukraine long ago began relevant works needed to create its own cyber security strategy. International experience in this field calls to create a system of global information exchange. According to the results of the researches cybercrime problems disturbs not only the state in a whole, but each individual inhabitant. Today, the fight against cybercrimes is one of the most relevant problems all over the world and in Ukraine in particular.

Analysis of recent researches and publications. The studies of contemporary issues on combating cybercrime reveal such leading scientists as Yu. Baturin, P. Bilenchuk, V. Viekhov, V. Golubev, M. Dikhtiarenko, B. Toleubekov, B. Worly, D. Shinder, D. Chyrylo.In practicetoo little attention is paid to the subject of cybercrime: in most cases the problems are experienced only in cases when crisis phenomena become significant threats to information and economic security, or even worse – is of irreversible character**.**

The goal of this scientific research is the study of conceptual aspects of cybercrime – security study dimension, reasoning of key indicators on cybercrime analysis and identification of diagnostic tasks in the field of information technologies. And also developing ways of combating cybercrime in the context of strengthening information and economic security.

Statement of main material. Based on the performed scientific studies we can say that cybercrime is an inevitable consequence of globalization of information processes. Simplicity, ease, anonymity, accessibility and time saving are the main directions that make information technologies attractive to mankind – could not but attract the attention of persons engaged in illegal activities.An increasing number of cyber crimes, continuous improvement of information technologies and as a result, new opportunities to «improve» tools of committing them create economic threats to global information networks and society as a whole. This growth is also an inevitable process because the legislative regulation of relations in the field of information technologies can neither be in advance of their development, nor march in step with it. It should be noted that in terms of penetration of cybercrime into social and public life, overcoming it is a fundamental factor on the way of Ukraine's entry into the global information space.

It is possible to guarantee effective counteraction toward this type of crimes only by applying integrated approaches to ensure information and economic security.Modern literary periodicals allows to interpret the following types of cybercrimes as illegal access, illegal interception, data interference, system interference, illegal use of computer passwords' devices, access code, or similar data.

It should be noted that the most common types of crimes involving the use of information technologies on the territory of Ukraine are: crimes in the sphere of computer and Internet technologies – 26%, crimes in the sphere of operation of electronic payments or payment cards – 16%, crimes in the sphere of telecommunications – 11% of crimes, in the sphere of computer technologies while committing traditional crimes – 47%. In addition, stealing of other persons' identification data has become a separate type of criminal actions, using which offenders gain access to other people's bank accounts, getting free internet and communications service providers. Such crimes are characterized by high level of technical support, latency, organization, availability of interregional and international relations [2]. Analysis of trends and dynamics of cybercrime in Ukraine leads to the conclusion that the regions with developed IT infrastructure, where the population widely uses telecommunication technologies (Dnipropetrovsk, Odesa, Lviv, Kharkiv) are considered the most common thing. Kyiv is the leader in this sphere, where almost 60% of all Ukrainian Internet audience is located. However, in recent years the number of solved cybercrimes in the sphere of IT-technologies in Ukraine almost did not change, although in the sphere of computer and Internet technologies the number of solved crimes increased in several times.

In the current contextcyber criminality has mostly organized and international character, and is based on rapid development and use of telecommunication means of messages.About 62% of cyber crimes are committed as part of organized groups, often on the territory of several countries. Cybercrime is also characterized by the relentless increasing and improving ways to commit crimes, each of them has many ways of committing [6]. We identify basic methods of committing cybercrimes:

1. Methods of direct access to computer technologies (operating system) and computer information related to criminal actions to destruct, block, copy computer information. There is a possible option of disruption of other computer equipment or computer network by issuing appropriate commands from the computer memory, which includes the plan of illegal actions. The above mentioned method has the most common character of applying in the crimes related to «white-collar crime». Among this category of cybercrimes the championship is occupied by persons directly involved in the production process: programmers, engineers, operators and others.

2. Methods of deleted (indirect) access to computer information is not in direct connection with another computer (network server) and available information contained therein. This connection can be made only through local networks or global systems such as the Internet.

3. Methods of creating, distributing on technical carriers harmful programs for computer. To this aspect we regard creation (writing) of unauthorized, viral programs that lead to harmful and dangerous consequences. The variety and number of such computer programs are numbered in tens of thousands of options, and they are modified depending on the category of persons who create them and for what subject they are created. Regarding the method of writing these illegal programs, there are also a fairly large number.

Researches of scientific issues allow identifying the main problematic aspects of combating cybercrime activity:

– need for global information exchange in real time regime;

– private and public sectors need financial incentives to improve cyber security;

– law enforcement authorities on combating cross-border cybercrime need more powers;

– it is needed to make methodological developments and implementing in technologies of combating cybercrime the best practices of international security institutions;

– existing diplomatic arrangement of global cyber agreements should become more addressed;

– to help the citizens it is needed to improve and extend the network of campaigns on informing population about methods of protection against cyber attacks [5].

This situation correlates with the above mentioned problems and demonstrates that increase of the level of information security in our country needs support and development.

Simultaneously it should be noted that the effective fight against cybercrime is impossible without the development of an integrated concept of criminological and statistical study of cybercrime, which includes general methodological, some methodical bases of cybercrime research, further prediction of its state and dynamics.

An important role in this process is played by information and analytical providing analysis of state and dynamics of cybercrime development, which allows controlling the internal connections between different types of crime and the dynamics' indicators of its development. This study is particularly important for understanding the mechanism of cybercrime formation and developing measures to prevent it.

Key place in the analysis of cybercrime is taken by an analysis of the status, structure and trends of the development. A qualitative and quantitative characteristic of cybercrime is the starting point of criminological research. Not knowing the scope of this type of cybercrime it is difficult to speak about the causes, consequences and necessary measures of combat and prevention.

In our opinion, a complete quantitative study of cybercrime is now quite complicated because of the lack of reliable statistical information on all of its actual indicators due to the high latency of certain types of crime.

Thus, the amount of financial losses caused by the actions of cybercriminals and the number of crimes committed by them are not exposed to real assessment due the fact that it is impossible to consider figures to be correct as they were obtained by processing the results of selective interviewing. By the way, this disadvantage may relate not only to data on losses, but also the number of recorded offenses. It is also unclear what percentage of the victims complainabout cybercrimes that have been committed against them. Although law enforcement authorities that combat cybercrime, appeal to these victims to report on the facts of crimes, it is believed that some of them, especially in the financial sector (i.e. banks), yet do not disclose such information because of the possibility to harm their reputation by spreading negative information of this kind. In addition, users that are exposed to such attacks do not always believe in the ability of law enforcement authorities to find guilty.

However, there is no doubt with the fact that the quantitative characteristics of cybercrime can give an idea of its main trends in one or another region for a certain period of time. In this regard, it seems relevant to analyze the main indicators, as well as the causes and conditions of cybercrime in the various spheres of society and economy that allow grounding the existence and further development of crime of this direction.

We have to admit that analysis of the parameters that characterize cybercrime can be carried out separately (analysis of individual indicators), and as well as within the generalized model (establishing links between individual indicators and analysis on the basis of selected links).

To analyze individual cybercrime indicators, in our view, the specifics of cybercrime formation, considering external factors (level of information technology, the number of registered Internet-users, etc.) must be taken into consideration. In this regard, the methods of analysis based on the use of the traditional system of mathematical statistics are ineffective and the adaptive methods of data processing used for work in terms of information shortage and inaccuracy come to the fore.

However, some peculiarities of the use of these methods in the analysis of cybercrime indicators should be mentioned:

– analysis of state and formed trends of crime development is based on statistical data that characterize a large number of committed and already investigated crimes of each type. With cyber crime the situation is not the same as with the other kinds: they are committed relatively seldom, and revealed and investigated – even less. Therefore, in our opinion, the existing information should be taken not as the truth, but only as the first approximation to further characteristics, which will appear after having accumulated significant experience;

– emergence of new types of cybercrime leads to the fact that the output rows of indicators are short. This problem severely limits the sphere of existing statistical methods applying [4].

Taking into the account the above said, statistical analysis of state and dynamics of cybercrime development should be carried out according to the following scheme, which we propose to consider according to Fig. 1.

It should be noted that the proposed approach greatly complicates the identification of the determining factors and peculiarities of modern cybercrime characteristic, which necessitates revision of criminological assessment of its main indicators, development of the system of criminal law and criminology measures of prevention and combating. As a result an analysis according to the proposed scheme will enable better control of internal connections between different types and indicators of cybercrime, which is especially important for understanding its mechanism and developing measures to prevent it.

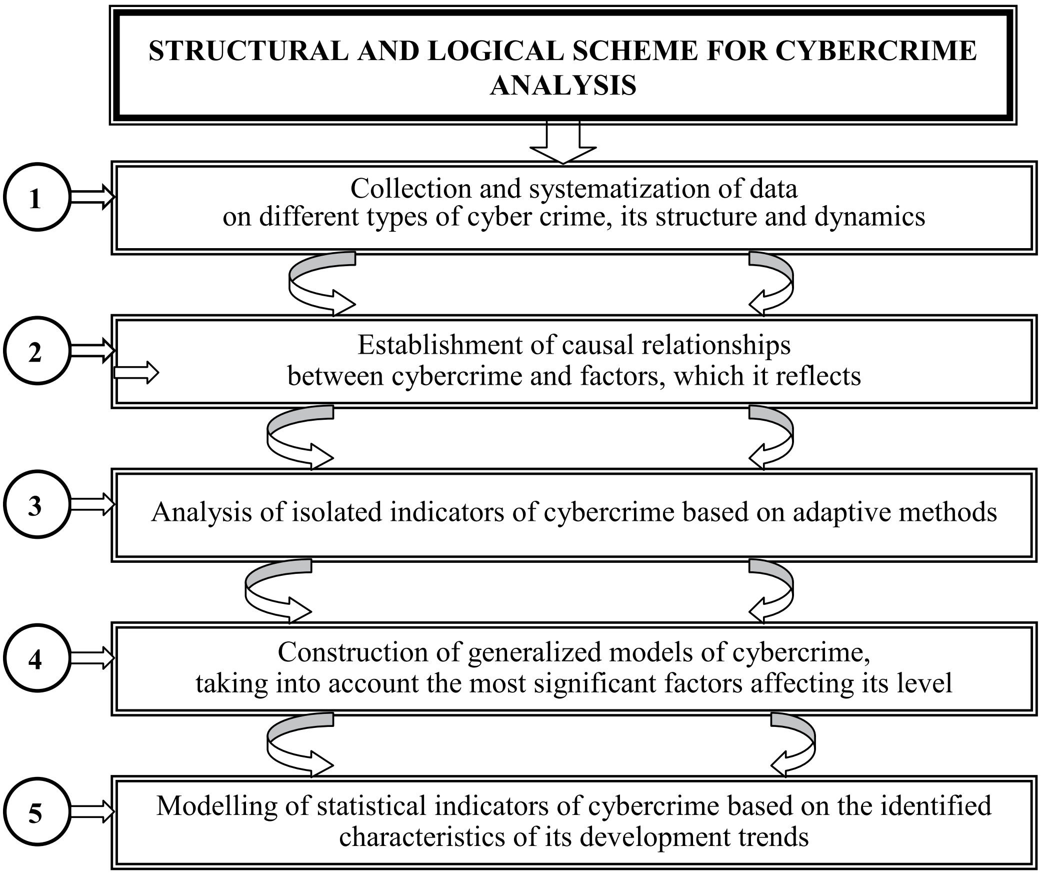
STRUCTURAL AND LOGICAL SCHEME FOR CYBERCRIME ANALYSIS
1
Collection and systematization of data on different types of cyber crime, its structure and dynamics
2
Establishment of causal relationships between cybercrime and factors, which it reflects
3
Analysis of isolated indicators of cybercrime based on adaptive methods
4
Construction of generalized models of cybercrime, taking into account the most significant factors affecting its level
5
Modelling of statistical indicators of cybercrime based on the identified characteristics of its development trends

Fig. 1. Structural and logical scheme for cybercrime analysis in terms of globalization processes [our own development]

It is impossible to leave aside diagnostic studies and identification issues arising during cybercrime. Considering the fact that diagnostic tasks according to aspectual characteristic are divided into the following ways:

– diagnostics of hardware and computer tools in the sphere of cybercrime: the definition of the kind (type, mark), the properties of the hardware as well as their technical and functional characteristics; the state of the hardware, the availability of breakdowns, defects; hardware carriers storage characteristics; reproduction of conditions environment, actual data of using hardware on the scene.

– diagnostics of program and computer tools in the sphere of cybercrime: establishing structural and quantitative characteristics of program and computer tools; characteristics of the actual state of software, specific programs and availability of their possible deviations; establishing a causal connection between the actions of the computer system user regarding the software and consequences that occurred.

– information and computer diagnostics in the sphere of cybercrime: characteristics and content of information stored in electronic computer carriers; identifying signs of interference and making changes into the information data; establishing mechanism and circumstances of the action based on the information held on computer carriers and their copies.

– computer and network diagnostics in the sphere of cybercrime: a general overview of computer network and its components; use of a typical computer-networking equipment and identifying signs of their deviations from established standards; causes of making changes in computer and network security and possible consequences of their use; establishing connection between the change in the computer-networking equipment and subjects that cooperate with this computer software.

We note that the widespread use of modern information technologies in society and state institutions puts forward solving of combating cybercrime problem as one of the major ones under the state regulation of national security system. In addition to the direct damage from possible cases of unauthorized access to personal information or information with restricted access its destruction or modification, informational support of the society can become a source of serious threat to information and economic security of the state [1].

In present unstable economic processes, nobody is surprised by daily media publications on new facts of proceedings of cybercrime cases, in particular on cases of fraud in the field of information technologies.

Since no state can protect itself by taking measures at a national level only, the necessary aspects for complex combating against cybercrime are: harmonization of the criminal legislation on cybercrime at international level; development at the international level and implementing into the national legislation procedural standards that allow to effectively investigate crimes in global information networks, receive, investigate and provide electronic evidence considering cross-border problems; adjusted law enforcement authorities cooperation while investigating cybercrime at the operational level; mechanism of resolving jurisdictional issues in cyberspace. At Fig. 2 there is a typical scheme of combating cybercrime in current market conditions.

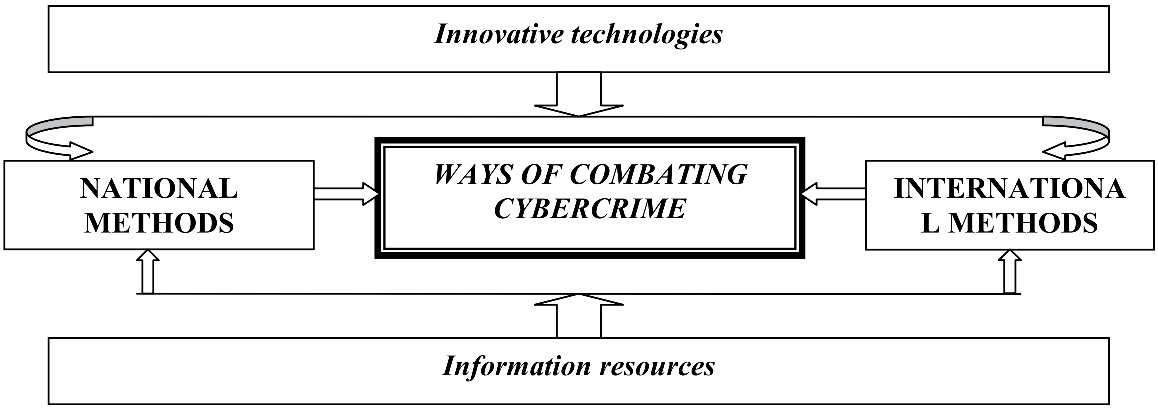

Fig. 2. Scheme of combating cybercrime in the context of economic and information security strengthening [our own development]

It is almost impossible to fight and control cybercrime at the level of an individual state. The adoption of international norms and standards should be accompanied by amendments to the national legislation of individual states. Coordination of the countries' efforts is important to ensure rapid response to the computer technologies development and approval of the appropriate standards.

For Ukraine this trend is in general positive: while its own strategy regarding cyberspace protection is just being developing, the extremely valuable is the opportunity to learn experience of the countries, which has been working in that direction for years. The process of combating development at national and international levels, as experience shows, is itself a complex problem.

But this is the only way to ensure security of users and state from electronic attacks, and also effectively investigate and pursue cybercrimes. As to strategy formation of combating cybercrime in the context of information and of economic security strengthening, the following vectors can be pointed out:

– building a governmental model aimed at cyber security ensuring;

– definition of adequate mechanism, mainly in the form of public-state partnership that will allow public and private interested party discuss and approve policies relating to cybersecurity problem;

– planning and defining the necessary policies and regulatory mechanisms, clear designation of roles, rights and responsibilities of the private and public sectors in combating cybercrime;

– defining objectives and methods of state capacity development and also necessary legislative framework for participation in the international fight against cybercrime;

– defining key informational infrastructures, including fixed assets, services and interdependencies;

– improving availability, reducing response time to incidents, developing disaster recovery plan and developing protection mechanisms for key information infrastructures;

– developing a systematic and integrated approach to the state risk governance;

– defining the objectives of information programs and approving them as priority, designed to instill users with new behavior models and patterns of work;

– prooving the necessity of a new educational program which focuses on training IT-specialists and professionals in the field of cyber security;

– developing international cooperation [3].

Conclusions. The results of this study lead to the conclusions that fruitful cooperation of the involved structures, both of public and international levels, which intends to fight the specified illegal phenomenon, is the way to reduce statistical data of cybercrime.

On the way to safe functioning of the subjects in national and global informational space the systematic approach to finding effective management decisions is extremely important. Dynamic development of cybercrime makes special demands on strategy and tactics of public policy of ensuring informationaland economic security forming, which should include a system of state and international measures.

Summarizing, we note that improving combating cybercrime activity will consist of the following directions: criminal and legal characteristics of cybercrimes; criminal and procedural aspects of combating cybercrime aimed at ensuring the collection of evidence in the investigation of computer crimes; international cooperation in criminal and procedural activity aimed at collecting evidence of cybercrime committing abroad.

So in environment where cyber threats are constantly emerging and evolving, we can not remain unprotected: situation formed in the world requires constant improvement of combating cybercrime methods and encourages state model building, aimed at ensuring cyber security of the country.

Literature

1. *Vivchar O. Peculiarities of assessment technologies usage in the management of financial and economic security of enterprises / O. Vivchar, A. Kolesnikov // Business Economics – Issue 4 (2), (October). Volume 51. «Palgrave Macmillan Ltd.», 2016. – Pages 393–398.*
2. *Кіберзлочинці щороку крадуть інформації на 400 млрд дол. [Електронний ресурс]. – Режим доступу : http://zik.ua/ua/news/2013/07/30/421804.*
3. *Орлов О. В. Актуальні напрями державної політики у сфері боротьби з кіберзлочинністю / О. В. Орлов, Ю М. Онищенко // Теорія та практика державного управління. – Вип. 3 (42) – 2013– с.1–6*
4. *Марков В. В. Статистичне дослідження показників кіберзлочинності: методологічний аспект / В. В. Марков // Право і безпека – 2013. № 2 (49), – с.136–139.*
5. *McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report [Електронний ресурс] // An Intel Company. – Режим доступу : \www/ URL:http://www.mcafee.com/us/about/news/2012/q1/20120120-01.aspx.*
6. *Украина – один из лидеров по количеству кибератак в мире [Електронний ресурс]. – Режим доступа : http://www.pravda.com.ua/rus/news/2013/03/8/6985180.*

Стаття надійшла до редакції 19.05.2017.