Visnyk of Dniprop'etrovsk University.
Ser. World Economy and International Economic Relations
Visny'k Dnipropetrovs'kogo Universy'tetu.
Ser. Svitove Gospodarstvo i Mizhnarodni Ekonomichni Vidnosy'ny'
Вестник Днепропетровского университета.
Сер. Мировое хозяйство и международные
экономические отношения
Visn. Dnipropetr. Univer. Ser. Svitove Gospodarstvo
i Mizhnarodni Ekonomichni Vidnosy'ny'. 2017, 9 (25), S. 3–17
doi 10.15421/181701

ISSN 2409-9228 (print)
www. dnu-wej.dp.ua

УДК 343.3+316.334.3
JEL: D21; F29; F42; K49; M14

Article info
Received
21.01.2017
Received in
revised form
06.03.2017
Accepted
10.03.2017

O. I. Vivchar*, O. I. Oliynychuk**

MODERN TRENDS OF CYBERCRIME IN THE CONTEXT OF ECONOMIC SECURITY, SOCIAL AND HUMANITARIAN ASPECTS

New challenges of cybercrime in the globalization conditions were noticed in the introduction of the article. The aim of the scientific research is to study of conceptual aspects of cybercrime – security study dimension, social and humanitarian aspects, to reason of key indicators on cybercrime analysis and to identify diagnostic tasks in the field of information technologies. And also the aim of the research is to develop the ways of combating cybercrime in the context of strengthening information and economic security. In research process both general and specific methods were used, namely, analysis and synthesis method; method of scientific abstraction; method of induction and the systems analysis method – in reasoning of the concept of combating cybercrime in the context of economic and information security strengthening. The results of the research describe aspects of economic security, social and humanitarian sides of cybercrime in modern conditions. Key problems of combating cybercrime activity in globalization conditions were considered.

There was noted 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, society 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.

The opinions of leaders of companies about cybercrime are very important for the research, so the poll on the subject was made. The owners or top managers of 15 business entities were selected as respondents. During the poll there were suggested to the respondents 10 questions related to their actions to combat cybercrime. The results of the investigation were shown in the article.

Scientific novelty of the research is the conceptual framework of combating cybercrime in current market conditions, which was grounded in the article. The practical significance of the results of the study is that the results of the study can be used for combating cyber at the macro- and the micro-level according to the suggestions, which were offered by the authors.

Key words: *cybercrime, cyber attack, cybercriminal, economic security, social and humanitarian sides of cybercrime.*

* Тернопільський національний економічний університет, Тернопіль, Україна;
E-mail: o.vivchar.84@gmail.com

** Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, Україна

О. І. Вівчар, О. І. Олійничук, О. Б. Погайдак

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ В КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА СОЦІАЛЬНО-ГУМАНІТАРНИХ АСПЕКТІВ

Розглянуто ключові проблемні аспекти боротьби з кіберзлочинністю в сучасних умовах глобалізації. Обґрунтовано основні показники аналізу кіберзлочинності, визначено завдання діагностики у сфері застосування інформаційних технологій, відображено підсумки опитування відповідних респондентів щодо кіберзлочинності, запропоновано напрями боротьби з кіберзлочинністю в контексті зміцнення інформаційно-економічної безпеки на макро- та мікрорівнях.

Ключові слова: *кіберзлочинність, кібератаки, кіберзлочинець, економічна безпека, соціально-гуманітарні аспекти кіберзлочинності.*

О. И. Вивчар, А. И. Олийнычук, О. Б. Погайдак

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ КИБЕРПРЕСТУПНОСТИ В КОНТЕКСТЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И СОЦИАЛЬНО-ГУМАНИТАРНЫХ АСПЕКТОВ

Рассмотрены ключевые проблемные аспекты борьбы с киберпреступностью в современных условиях глобализации. Обоснованы основные показатели анализа киберпреступности, определены задачи диагностики в области применения информационных технологий, отражены итоги опроса соответствующих респондентов по киберпреступности, предложены направления борьбы с киберпреступностью в контексте укрепления информационно-экономической безопасности на макро- и микроуровне.

Ключевые слова: *киберпреступность, кибератаки, киберпреступник, экономическая безопасность, социально-гуманитарные аспекты киберпреступности.*

Introduction

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 disturb 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 many scientists. O. O. Yona and N. F. Kazakova have shown the current situation in the world of cybercrime that requires constant improvement of methods of struggle (Yona, Kazakova, 2013). V. M. Strukov and V. V. Torzhnyk have suggested the ways of cybercrime prevention in the context of the state information security (Strukov, Torzhnyk, 2013). V. A. Holubev has conducted a cybercrime analysis in the sphere of economic security (Holubev, 2013). The features of transnational cybercrimes were considered by V. M. Babakin (Babakin, 2011). The article of V. V. Markov is devoted to the analysis of methodological characteristics of quantitative (statistical) characteristics of cybercrime in Ukraine (Markov, 2013). The characteristic signs of subculture of cyber-

criminals were defined by B. V. Dziundziuk (Dziundziuk, 2013). International cooperation in the fight against cybercrime was investigated by O. V. Orlov, Iu. M. Tyshchenko (Orlov, Tyshchenko, 2013). Simultaneously in practice too 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.

Is to study of conceptual aspects of cybercrime – security study dimension, social and humanitarian aspects, to reason of key indicators on cybercrime analysis and to identify diagnostic tasks in the field of information technologies. And also the aim of the research is to develop the ways of combating cybercrime in the context of strengthening information and economic security.

Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government (Cybercrime). 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.

Contemporary hacker subculture has a criminal base, because it can be defined as a set of ideas, values, traditions, rules of conduct aimed at life organization, the purpose of which is to commit computer crimes, concealment and evasion of responsibility. Thus the value complex of the subculture serves to legitimize and popularize the idea of hacking in society, which is why a person who shares the values of hackers is ready to make the Internet crime or endorses crimes committed by others (Dziundziuk, 2013).

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 (Kiberzlochyntsi). 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 (Dnipro, 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 context cyber 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. The Table 1 contains information about top-10 target countries and top attacking countries.

Data of the Table 1 shows that China, USA, France are both the target and attacking countries.

It should be noted that cybercrime is characterized by the relentless increasing and improving ways to commit crimes, each of them has many ways of committing (Ukraine). The basic methods of committing cybercrimes were identified:

Table 1. Top-10 target and attacking countries, 2017

Ranking	Top target countries	Ranking	Top attacking countries
1	Philippines	1	China
2	India	2	USA
3	Turkey	3	France
4	Brazil	4	Finland
5	France	5	Sweden
6	China	6	Italy
7	USA	7	Netherlands
8	Mexico	8	United Kingdom
9	Cambodia	9	Singapore
10	Indonesia	10	Colombia

Source: Live cyber attack threat map (16/2/2017).

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 (McAfee and Security).

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 de-

velopment, 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 complains about 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.

Cybercrime has significant manifestations in the economic sphere and consequences both on macro- and micro-level, because it is a cause of great damage to individual subjects, including business subjects (Oliynychuk, 2016). Recently there has been a significant increase of the incidence of unauthorized interference into the information systems of different spheres enterprises. The attackers block of using software that makes it impossible to follow the work of the various departments of the enterprise. This often leads to problems with contractors, controlling authorities, because in this situation the ability accounting and analytical service of company to form information and in particular report information is lost. Also it is impossible to pass in time the financial reports to the appropriate authorities, and this, in turn, leads to penalties for breach of taxpayer discipline.

The opinions of leaders of companies about cybercrime are very important for the research so we have made the poll on the subject. The owners or top managers of 15 business entities of different economy sectors and regions of Ukraine, including manufacturing, trading, insurance, services etc. were selected as respondents. During the poll

there were suggested 10 questions to the respondents with short answers (Yes or No) related to their actions to combat cybercrime:

1. Has your business entity ever been under the cyber attack?
2. Do you think that in the case of cyber attack should immediately contact with the law enforcement authorities?
3. Do you think that the appeal to law enforcement authorities will have positive results for solving of your problem?
4. Do you think the staff of the law enforcement authorities is high qualified for combating of cybercrime?
5. Do you think that in the case of cyber attack should go to the contact with the attacker (attackers) to solve your problem?
6. Do you believe that your business entity is reliably protected from cyber attacks?
7. Do you think that the threat of cyber attacks is related with the specifics of the company activity?
8. Do you believe that it is possible to identify quickly and bring to justice the cybercriminals?
9. Do you believe that current legal support is sufficient for the effectively detection and prosecution of cybercriminals?
10. Do you think that there are effective ways to overcome cybercrime?

The Table 2 contains information about answers the question.

The results of our investigation are very interesting. So the first question provides information about the amounts of respondents, whose business entity have ever or never been under the cyber attacks. This data is shown in Figure 1.

Table 2. The results of the poll*

Business entities / Questions	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***	***13***	***14***	***15***
1.	–	–	–	+	–	+	–	–	–	+	–	+	+	–	–
2.	+	+	+	_	+	+	–	+	+	+	+	+	+	+	–
3.	–	–	+	_	–	+	–	+	–	+	+	–	–	+	–
4.	+	–	–	_	–	+	–	–	–	–	+	–	–	–	–
5.	–	–	–	_	–	–	–	–	–	+	+	–	–	–	+
6.	+	+	–	_	–	+	–	–	–	–	–	–	+	+	–
7.	–	+	–	_	–	+	+	+	–	–	+	+	–	+	+
8.	+	–	–	_	+	+	+	–	–	–	+	+	+	+	–
9.	–	–	+	+	–	–	+	–	–	–	–	–	–	–	–
10.	–	+	–	+	–	+	+	+	–	–	+	+	+	–	+

*Yes "+", No "–"

Source: compiled by the authors (February 2017).

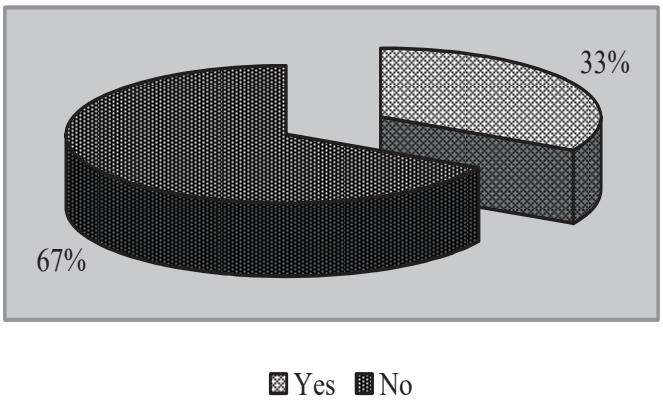

Fig. 1. Shares of business entities, which have (have not) been under the cyber attacks (developed by the authors)

Figure 1 demonstrates that majority of the respondents have never been under the cyber attack. Certainly it is good indicator.

The results of the answers the other questions are the next:

- 80% of the respondents think that in the case of cyber attack should immediately contact with the law enforcement authorities, but only 40% of respondents think that the appeal to law enforcement authorities will have positive results for solving of the problem;
- only 20% of the respondents think the staff of the law enforcement authorities is high qualified for combating of cybercrime;
- however 20% of the respondents think that in the case of cyber attack should go to the contact with the attacker (attackers) to solve the problem;
- 33% of the respondents believe that their business entities are reliably protected from cyber attacks;
- 53% of the respondents think that the threat of cyber attacks is related with the specifics of the business entity activity;
- 53% of the respondents believe that it is possible to identify quickly and bring to justice the cybercriminals;
- 20% of the respondents believe that current legal support is sufficient for the effectively detection and prosecution of cybercriminals;
- 60% of the respondents think that there are effective ways to overcome cybercrime.

Based on the results of the poll we have made the next conclusions:

1. Fortunately only 1/3 of the respondents faced with the cyber attack and knows the conclusions of unauthorized interference into the information systems;
2. he vast majority of the respondents prefer to contact with the law enforcement authorities, but more than half of respondents think that the appeal to law enforcement authorities will have not positive results for solving of the problem. Besides the vast majority

of the respondents do not believe that current legal support is sufficient for the effectively detection and prosecution of cybercriminals. This is the evidence of negative image of the domestic law enforcement authorities and law system in general;

3. In terms of total distrust to law enforcement authorities, which has turned into a chronic in Ukraine, 20% of owners and top managers of investigated business entities prefer to independently solve problems through the contact with criminals and fulfillment of their illegal requirements, rather than appeal to the appropriate law enforcement structures;
4. Nearly half of the respondents do not think that the threat of cyber attacks is related with the specifics of the company activity. They say any company can be target of cybercriminals;
5. Nearly half of the respondents do not believe that it is possible to identify quickly and bring to justice the cybercriminals. This is the testimony of public understanding of high level of cybercrime latency;
6. Little more than half of the respondents believe that there are effective ways for overcoming of cybercrime. That indicates the presence of positive public expectations to overcome cybercrime.

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 approxima-

tion 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 (Markov, 2013).

Given the above-mentioned 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. 2.

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.

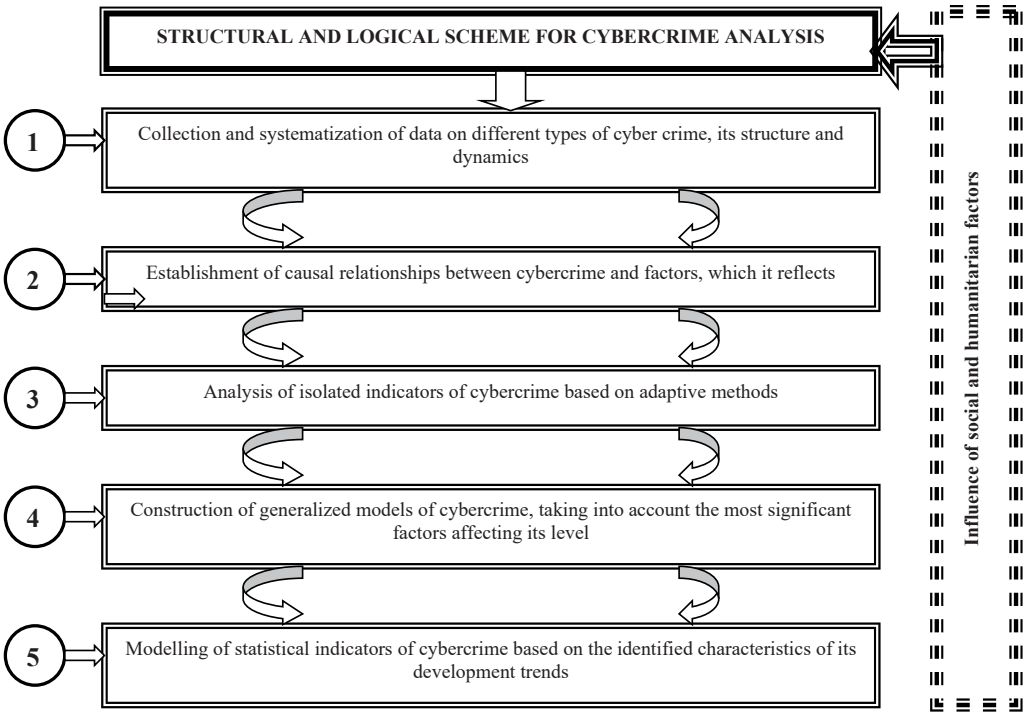

Fig. 2. Structural and logical scheme for cybercrime analysis in terms of globalization processes (our own development)

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 (Vivchar, Kolesnikov, 2016).

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. 3 there is a typical scheme of combating cybercrime in current market conditions.

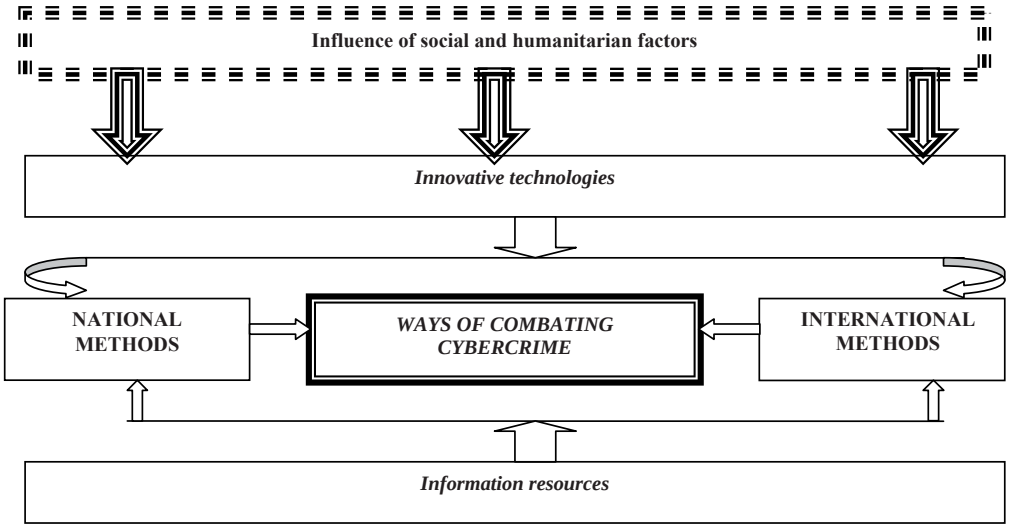

Fig. 3. Scheme of combating cybercrime in the context of economic and information security strengthening (our own development)

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;
- proving the necessity of a new educational program which focuses on training IT-specialists and professionals in the field of cyber security;
- developing international cooperation (Orlov, Onyshchenko, 2013).

Also it is necessary to develop the set of measures to prevent cyber attacks at micro-level. The leaders of those business entities that have experience of unauthorized interference into the information systems recognize the significance of its effects. They understand their mistakes, which have made the cyber attacks successful. Based on their experience we can identify the following ways to combat cyber attacks:

1. Use only licensed software, especially licensed anti-virus software;
2. For the purpose of minimizing the consequences of cyber attacks to make regular duplication of information and storing it in different information carriers;
3. Use the services of highly skilled IT-specialist (IT-specialists), who has (have) to serve the information needs of the business entity and will be responsible for their cyber security. If the company has large activity, the IT-specialist (IT-specialists) can be as a part of the personnel. If the company is small, should use the services of the IT-specialist on a contractual basis;
4. Payment of highly skilled IT-specialist should fully comply with his qualification. Only in this case it is possible to require him to take responsibility for the consequences of cyber attacks for the enterprise;
5. If the IT-specialist works like a staff of the enterprise, should send him to the training for review of recent manifestations of cybercrime and the ways of combating. If the IT-specialist, serving

Conclusions the company works on a contractual basis, it is necessary to require him to submit evidences of regular training.

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 informational and 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.

References

Babakin, V. M. (2011). Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv [International Cooperation Singularities at Fact-finding of Cybercrimes]. Forum prava, 4, 27–30 (in Ukrainian). Cybercrime. [online] Available at: https://www.britannica.com/topic/ cybercrime.

Dziundziuk, B. V. (2013). Osoblyvosti subkultury kiberzlochyntsiv [Features of cybercriminals' subculture]. Teoriia ta praktyka derzhavnoho upravlinnia, 2, 333–339 (in Ukrainian).

Holubev, V. A. (2013). Analiz kiberzlochynnosti u sferi ekonomichnoi bezpeky [Analysis of cybercrime in the economic security sphere]. Information Technology and Security, 1, 26–32 (in Ukrainian).

Kiberzlochyntsi shchoroku kradut informatsii na 400 mlrd. dol. [Cybercriminals steal information annually to $400 billion]. [online] Available at: http://zik.ua/ua/news/2013/07/30/421804.

Live cyber attack threat map (2017). [online] Available at: https://threatmap.checkpoint.com/ThreatPortal/livemap.html.

Markov, V. V. (2013). Statystychne doslidzhennia pokaznykiv kiberzlochynnosti: metodolohichnyi aspekt [Statistical research of cybercrime's indicators: methodological aspect]. Pravo i bezpeka, 2(49), 136–139 (in Ukrainian).

McAfee and Security & Defence Agenda (SDA) Unveil Global Cyber Defense Report. [online] Available at: http://www.mcafee.com/us/about/news/ 2012/q1/20120120-01.aspx.

Oliynychuk, O. I. (2016). Pravovi osnovy protydii ekonomichnii zlochynnosti: navchalnyi posibnyk [Legal basis for combating economic crime]. FO-P Shpak V. B., Ternopil (in Ukrainian).

Orlov, O. V., Onyshchenko, Iu. M. (2013). Aktualni napriamy derzhavnoi polityky u sferi borotby z kiberzlochynnistiu [Recent trends of state policy in the sphere of fight against cybercrime]. Teoriia ta praktyka derzhavnoho upravlinnia, 3(42), 1–6 (in Ukrainian).

Orlov, O. V., Tyshchenko, Iu. M. (2013). Mizhnarodna spivpratsia u sferi borotby z kiberzlochynnistiu [International cooperation in the sphere of fight against cybercrime]. Teoriia ta praktyka derzhavnoho upravlinnia, 4, 17–23 (in Ukrainian).

Strukov, V. M., Torzhnyk, V. V. (2013). Profilaktyka kiberzlochyniv v konteksti informatsiinoi bezpeky derzhavy [Prevention of cyber crime in the context of the state information security]. Systemy obrobky informatsii, 2, 204–206 (in Ukrainian).

Ukraina – odin iz liderov po kolichestvu kiberatak v mire [Ukraine is one of the leaders in the number of cyber attacks in the world]. [online] Available at: http://www.pravda.com.ua/rus/news/2013/03/8/6985180.

Vivchar, O., Kolesnikov, A. (2016). Peculiarities of assessment technologies usage in the management of financial and economic security of enterprises. Business Economics, 4(2), 393–398.

Yona, O. O., Kazakova, N. F. (2013). Svitovi tendentsii borotby z kiberzlochynnistiu [Global trends fight cybercrime]. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia, 15(1), 59–61 (in Ukrainian).