UDC 343.131

SHORTCOMINGS AND SUGGESTIONS ON IMPROVING THE LEGAL COMPONENT OF CRIME COMBATING MECHANISM IN THE FIELD OF ICT

Drobozhur R.R., Malyshev M.A.
National University «Odessa Law Academy»

This research is devoted to the analysis of Ukrainian legislation in the sphere of crime combating in the cyber-security field as well as studying of practice of law-enforcement authorities in this sphere. An effective mechanism to combat crime in the sphere of information and communication technology (ICT) provides integrated use of three approaches – engineering, organizational and legal. Legal approach is meant fundamental and constitutive among these three approaches and its mechanisms are applied complexly with organizational and engineering aspects. The sense of legal approach lays in creating normative basis for realization of other two approaches. Consequently, it is the analysis of the legislative framework of crime combating in the sphere of ICT makes it possible to explore the weaknesses of modern mechanisms of ensuring cyber-security more deeply and identify the root cause of the problems of their inefficiency. The article presents detailed analysis of national legislation in the information field in general and in the field of cyber security in particular, reveals some of its weaknesses and presents proposals for the elimination of these shortcomings.
Keywords: cybercrime, cyberspace, information and communication technologies, information security, information protection.

Formulation of the problem. New historical phase of civilization – the information society – is gradually quickening, bringing not only positive but also negative trends and phenomena. According to statistics, Ukrainians increasingly use all the achievements of the information age and try to use all the features of electronic interaction. Moreover, it is safe to say that today there are no public or private institutions, which would not use modern information and communications technologies – computer networks, databases, automated system for ensuring production lines etc.

However, further development of modern information technologies and expanding of the field of use of modern computer technologies gave a start to the emergence of specific, complex type of illegal activities where technical equipment and computer information are subjects to unlawful infringement or where computer equipment is an instrument of its commission itself. We are talking about crimes in the sphere of information and communications technologies (ICT) or "computer crimes" (cybercrimes).

However, even a superficial analysis of the Ukrainian cyber-security sphere gives reason to talk about a number of important problems that hinder the creation of an effective system to counter threats in cyberspace. These problems include primarily: terminological uncertainty, lack of proper coordination of relevant agencies' activity, Ukraine's dependence on foreign software and hardware, some difficulties concerning staff recruitment to the relevant departments. Despite the existence of a number of legal documents on cyber security problems of the state, which are in force, they do not cover the entire spectrum of threats to the cyber-security of the state.

Analysis of recent researches and publications. Certainly, the phenomenon of cybercrime was not left unnoticed by scientists and different branches of law. For example, dissertation researches on the criminal aspects of crime in the field of information technologies are scientifically substantiated by national researchers: D. S. Azarov, N. V. Karchevsky, M. V. Pluhatyr, N. A. Rosenfeld etc. A significant contribution to the study of investigation and combating computer crimes made such leading scientists T. V. Averyanova, B. V. Andreev, Y. Baturin, R. S. Belkin, P. D. Bilenchuk, O. A. Baranov, M. S. Vertuzayev, T. V. Varfolomeyeva, O. H. Volyevodz, V. A. Golubev, V. S. Tsimbalyuk and others.

Highlighting of previously unsolved aspects of the problem. In our opinion, despite the theoretical and practical importance of conducted and published research, not enough attention is paid to the study of the shortcomings and problems of combating cybercrime in Ukraine.

The purpose of the article. The purpose of the article is to examine possible solutions of problems of crime combating mechanisms functioning in the field of ICT. For this, it is necessary to identify deficiencies in the legal, organizational and institutional mechanisms of combating cybercrime in Ukraine and, accordingly, make proposals to eliminate shortcomings in the conceptual and terminological aspects of law in Ukraine in the field of cyber-security.

Statement of the basic material. Examination of Ukrainian information legislation, which was repeatedly carried out in recent years, including representatives of the OSCE, indicates that the legislative and normative basis of functioning of information sphere in Ukraine generally meets European standards. Although the formal side of things does not cause significant concern, there is an urgent problem of non-compliance of all the subjects of information relations with established legal norms , in particular – public authorities at all levels. The level of legal culture of Ukrainian citizens makes consider the situation from a completely different side to the European Union countries [1].

An important problem is certain inconsistency of national legal policy in the information sphere. A large number of legislative acts to address specific tactical tasks, meet personal or commercial interests are often adopted without considering the strategic goals and real conditions in Ukraine.

For example, the attempts of revising legislation to permit advertising of alcohol and tobacco were very demonstrative.

Much of the issues in the information sphere's functioning is legally unsettled. This applies to infrastructure problems, media activity, information and analytical agencies, etc. As an example, let us analyze legislative provision of such an important component of national information policy as information transparency and openness in the functioning of state government and services. Ukraine has formed a legal framework to ensure transparency of state authorities. First of all, it is about the Constitution of Ukraine (art. 3, 32, 57, etc.), the law "On information", "On the print media (the press) in Ukraine", "On Television and Radio", "On the information agencies", "On State service "and so on.

The main drawback of the current legislation it is passive nature – it was declared only the necessity of ensuring transparency of public authorities in response to the appeals of citizens or the media. To obtain certain information, a citizen has to prepare and submit to the institution a request and expect a response within a month [2, p. 113]. As you can see from this, public authorities are, in fact, absent in the information space. Cases when the policy of the State is not reported to public by itself but its opponents are frequent too. Then, as the legislation of democratic countries means active information activity, mandatory reporting of the state authorities to the public, regardless whether the appeals or requests for the provision of any information were or not, obligatory, maybe even a bit too active, informing citizens about the ongoing activities of public authorities.

Another disadvantage of the current Ukrainian legislation, particularly in the information sector is its vagueness, a certain blurring of wording. In fact, there is no identification of specific mechanisms for promulgation information, particular documents that have to be published. The terms of this activity has not been set yet, the legal norms of strict appliance concerning financial and staff provision [3].

The absence of legal regulation of international information systems, for example – Internet, is a significant problem. In particular, the lack of appropriate regulations creates certain problems for Internet media and promotes their use in destructive purposes. The development of information infrastructure requires appropriate legislative support.

Returning to the issue of imperfection of mechanisms for combating crime in the ICT sphere, it should also be noted that the use of such familiar and rather widespread notion as "cybercrime" to characterize a specific group of crimes attributed to the so-called "cyber area" (crimes in information technology sphere, computer technology systems and networks) needs some theoretical legal understanding, in the first place – conceptual and terminological analysis [4, p. 150]. The term "cyber-crime" has gained rather wide usage in the post-Soviet space without legal content. Not only the problem of setting the ratio of "cybercrime" with such concepts as "computer crime", "crime in the sphere of computer information", "crime in the field of computers usage", "crime in the sphere of information technology", or with legal concept of " crime in the sphere of electronic computers (computer) systems and computer networks and telecommunication networks usage" remains unsolved, but also conceptual definition of the place of "cybercrime" in the system of illegal acts provided by national law. All this raises serious doubts about relevance and possibility of legal defining of cybercrime and its introduction as a separate type of crime by criminal law. The way of solving this problem is thorough general theoretical understanding of the content of the concept of "cybercrime", which is provided the prefix "cyber", taking into account axiological, etymological, semantic features, as well as the history of emergence and development of the cybercrime phenomenon. The said issue relates to a number of problems of forming the concepts and terminology apparatus of cyber security field and it must be resolved comprehensively [5].

Another manifestation of conceptual and terminological problem is loan nature of the "cybercrime" concept with a certain content laid on it by international legal acts, including the Convention on cybercrime, created by states with different types of legal systems and different understanding of the "crime" concept. The understanding of cybercrime provided by them is quite generalized and abstracted from the legal system of particular state and cannot fully meet its features that additionally raise the problem of the legal implementation [6, p. 434].

Taking into account high level of latency of cybercrime, which causes secrecy of real volumes of its negative consequences, the possibility of using such criteria as the amount of public damage or degree of public danger as determining during the classification of offenses in the cyber area is ineligible. Besides, the issue of separating "cyber offense" as the type of crime was almost never considered [7, c 75] leaving out of a public-legal response the significant number of actions that does not cause much social harm alone and, accordingly, may not be qualified as "crimes" but in the mass create a public danger. Among them, it may be a latent form of cybercrime, which also remains without adequate response.

The last problem can be further intensified by the novels of the Criminal Procedure Code of Ukraine that initiates the introduction of a new kind of offenses for the legal system for Ukraine – criminal offense, which in the future will have its own regulation of substantive criminal law.

Possibilities to use methods of legal impact on the consciousness of individuals in Ukraine are quite limited today, first, because of low level of legal and information culture of citizens, which do not rely on internal motivation to appropriate (lawful) behaviour and proper protection of their constitutional rights, and secondly, because of transnational nature of cybercrime, which may go beyond the jurisdictional limits of a separate state. It is obvious that only the influence on the behaviour of individuals has the real potential of effectiveness under such conditions. This gives a special value to law enforcement components of cybercrime combating, i.e. the system of efficient law enforcement norms, especially criminal, created by the unified international standards, and

effective activity law enforcement and judicial authorities of the State and the relevant international organizations regarding the application of these rules [8, p. 180].

The solution of the mentioned problems can be a step towards adequate legal perception of the phenomenon of "cybercrime", determination of necessity and extent of its legal implementation, and consequently, the harmonization of the national legal framework aimed at combating cybercrime.

This inconsistency in terms defining applies not only to the concept of "cybercrime". Thus, in the Law of Ukraine "On the fundamentals of National Security of Ukraine", it is mentioned "computer crime" and "computer terrorism", but none of these terms has its definition neither in this nor in other laws. In the Law of Ukraine "On Combating Terrorism", the concept "computer terrorism" was not mentioned at all, and those elements that can be referred to it are prescribed as part of the concept "technological terrorism". In the "National Security Strategy of Ukraine" (version from February 12, 2007 № 105/2007) computer threats were not mentioned at all, while "cyber security" – only in the context of the need of "development and implementation of national standards and technical regulations of ICT, harmonized with the relevant European standards, including requirements of the Convention on Cybercrime ratified by Verkhovna Rada of Ukraine". However, the new published edition of "National Security Strategy" (2011) already uses the term "cyber-security". The "Doctrine of Information Security of Ukraine" (repealed in 2014) also mentioned "computer crime" and "computer terrorism", but without any explanation or reference to such explanations. Therefore, we can say the domestic legal framework in the field of information (cyber) security uses the terms that have not any definitions.

There is also an urgent problem of the lack of a unified national system of combating cybercrime, coordination its activities and legal regimentation of areas of responsibility between agencies, procedures and means of cooperation as the most comprehensive response to the threats to cyber-security of the state and significant work to prevent such crimes [9].

In order to solve these problems and disorder of the legal framework, public security institutions carried out a whole number of measures. The basis for these was the decision of the National Security and Defence Council of Ukraine of 17 November 2010 "On the challenges and threats to the national security of Ukraine in 2011" [10, p. 41], which was approved by the Decree of the President of Ukraine on December 10, 2010 № 1119/2010.

Another problem of national legislation on cyber security, as stated above, is imperfection and inconsistency of concepts and terminology apparatus. National Institute for Strategic Researches sent a number of official requests to key agencies (Security Service of Ukraine, the Foreign Intelligence Service, General Intelligence Directorate Ministry of Defence of Ukraine, Ministry of Internal Affairs) and scientific institutions (Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Interdepartmental scientific Research Centre for Combating Organized Crime of the National Security and Defence Council of Ukraine) relating to information (including – technological components) of state security to determine approaches to key terms in this field.

After the analysis of the responses, were formed definitions of key terms in the field of cyber-security that can become the basis of developed legal framework in the field of protection of cyberspace of the state.

Terms and definitions proposed by the National Institute of Strategic Researches for inclusion in the draft of the law "On cyber security of Ukraine":

1. Cyberspace – objects of information infrastructure governed by information (automated) systems of management and information, which circulates in it.

2. Cyberspace of the state – objects of information infrastructure of the state governed by information (automated) systems of management and information, which circulates in it.

3. Information infrastructure – a set of objects of telecommunication systems of all forms of ownership.

4. Information infrastructure – a set of objects of telecommunication systems of all forms of ownership located in the state or accessed from the state.

5. Critical information infrastructure of the state – a set of information and telecommunication systems of the state and the private sector that ensure the functioning and safety of strategic institutions of the state and safety of citizens.

6. Cyber-security – the state of cyber security as a whole or individual objects of its infrastructure from risks of foreign cyber influence (cyber-attacks), at which it is provided their sustainable development, and early detection, prevention and neutralization of real and potential threats to personal, corporate and / or national interests.

7. Cyber Defence – a set of methods and measures of organizational, legal and technical nature to ensure cyber-security.

8. Cyber-attack – deliberate actions implemented in cyberspace (or using technical capabilities) that lead (can lead) to achieve unauthorized purposes (violation of the confidentiality, integrity, authorship and availability of information, destructive information and psychological influences on consciousness, psychological and mental state of citizens).

9. Cybercrime – criminal act, responsibility for which is envisaged by criminal law, that is established (being established) in cyberspace (or through its technical capabilities) and bears the danger to society.

Separation of "cyber-terrorism" as an independent concept is one of the most controversial issues in cyber-security field. This is reasoned by, firstly, extraordinary politicization of the concept, and secondly, by the necessity of defining its keynote settings, so it would be impossible to take conventional computer crime or hooliganism under their action. In modern Ukraine, the basis of countering terrorism and combating its manifestations is the Law of Ukraine "On Combating Terrorism" [12, p. 180]. In this law, terrorism is defined as "socially dangerous activity that lays in conscious, purposeful

use of violence by hostage-taking, arson, murder, torture, intimidation of the population and the authorities or any other encroachment on the life or health of innocent people or threats to commit criminal acts in order to achieve criminal goals". Among the proposed definitions of cyber-terrorism, the offer of Security Service of Ukraine in the best way correspond the current version of the Law of Ukraine "On Combating Terrorism». However, this definition requires some refinement in its final form and may be represented as follows:

"Cyber-terrorism – socially dangerous activity, carried out in cyberspace (or using technical capabilities) with a terrorist purpose and lays in conscious, purposeful intimidation of the population and the authorities or any other attacks on human life and health". This definition should be introduced to the Law of Ukraine "On combating terrorism", removing from the definition of "technological terrorism", the words "... usage of means of electromagnetic action, computer systems ...". In addition, the Security Service of Ukraine has proposed to allocate separate series of definitions that will distinguish cyber-terrorist acts of other criminal acts: cyber offence, cyber espionage, cyber diversion [13].

Conclusions and suggestions. To improve the mechanisms of combating crime in the field of ICT it is necessary, first – to develop a modern regulatory support of this sphere, which would correspond to the realities of scientific and technological progress of mankind. Secondly, it is urgent to revise the existing legislation on cyber-security. It is important to provide normatively a system to prevent cybercrime and raise the level of people's knowledge of specific forms of cybercrime and means of protection against them. It appears appropriate to ensure the full integration of Unified State System of Combating Cybercrime (USSCC) into the legislation, to create it under the Decree of the President of Ukraine "On the challenges and threats to the national security of Ukraine in 2011" dated December 10, 2010 № 1119/2010 according to the necessity.

Meanwhile the Security Service of Ukraine proposed successful, in our view, model of the organizational structure of the system that should operate like a single system of prevention, response and suppression terrorist attacks and minimizing their consequences, the provisions of which was approved by the Cabinet Ukraine dated 15 August 2007 №1051.

In particular, the USSCC proposed to introduce the following functional elements:

· national system of monitoring and responding to security threats in cyberspace (provides quick identification of the attacker and measures for localization harm caused by malicious actions);

· the system of measures for the levelling of threats and vulnerabilities of cyberspace and cybercrime investigation;

· national system of critical information infrastructure protection

It should be noted that mentioned judgment of NSDC "On the challenges and threats to the national security of Ukraine in 2011" in April 2014 was cancelled [11, p. 39] after the review of its performance, though there are no reasons to talk of its realization.

Therefore, summarizing the results of the analysis of the problems of existing legislation and terminological uncertainty in the area of cyber-security, we can draw the following conclusions:

1. Despite the existence of a number of legal documents on cyber-security problems of the state, they do not cover the entire spectrum of threats to the cyber-security of the state.

2. The existing regulatory framework has not definition (and therefore specific forms of protection, response and responsibility are not implemented) of key elements of state infrastructure against cyber-attacks.

3. Terminological field of cyber security areas of the state remains fragmented, which makes impossible the formation of effective legal documents of combating cyber threads.

4. There are not established definitions of key terms ("cyberspace", "cyber-attack" "cyber-security" "cyber protection", "cyber-war", "cyber-terrorism", "cyber weapon", "cyber-infrastructure", "critical cyber-infrastructure") that can effectively be used in law enforcement practice.

5. The only national system of combating cybercrime that has appropriate regulatory support is still under development and needs much more improvements.

References:

1. Kudriavtseva S.P. Mizhnarodna informatsiia: Navchalnyi posibnyk [Electronic source] / S.P. Kudriavtseva, V.V. Kolos // K.: Vydavnychyi Dim «Slovo». – 2005. – Access mode: http://pulib.if.ua/part/9895.
2. Zasoby masovoi komunikatsii yak sub'iekt realizatsii derzhavnoi informatsiinoi polityky Ukrainy v sferi oborony: polityko-pravove rehuliuvannia / Iu.V. Turchenko // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. [Electronic source] – 2013. – Vyp. 43. – S. 113-119. – Access mode: http://nbuv.gov.ua/j-pdf/Znpviknu_2013_43_20.pdf
3. Shpenov D.Iu. Problemy stanovlennia ta perspektyvy rozvytku pravovoho rehuliuvannia vidnosyn v informatsiinii sferi / D.Iu. Shpenov // Forum prava. – 2011. – № 3. – S. 894-898 [Electronic source]. – Access mode: http://www.nbuv.gov.ua/e-journals/FP/2011-3/11sdjvsc.pdf
4. Karchevskyi M.V. Zlochyny u sferi vykorystannia kompiuternoi tekhniky : navch. posib. / M.V. Karchevskyi ; Luhanskyi derzh. un-t vnutrishnikh sprav. – Luhansk : RVV LDUVS, 2006. – 192 s.
5. Melnyk S.V., Tykhomyrov O.O., Lienkov O.S. Do problemy formuvannia poniatiino-terminolohichnoho aparatu kiberbezpeky // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka, Vyp. 30 [Electronic source]. – Access mode : http://www.nbuv.gov.ua/portal/natural/Znpviknu/ 2011_30/Zbirnik_30_28.pdf
6. Tykhomyrov O.O. Pravovi problemy protydii kiberzlochynnosti na transporti / O.O. Tykhomyrov // Transportne pravo v KhKhI stolitti: [Materialy III Mizhnarodnoi naukovoi konferentsii, Kyiv, NAU, 21 liutoho 2013 r.] – K. : Komp'iuterpres, 2013. – 434 s.

7. Tykhomyrov D.O. Do problemy rozmezhuvannia kiberzlochynu i kiberprostupku / D.O. Tykhomyrov // Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy : zb. materialiv nauk.-prakt. konf., m. Kyiv, 22 bereznia 2011, Chastyna 2. – K. : Vyd-vo NA SB Ukrainy, 2011. – S. 75-77.
8. Tykhomyrov O.O. Kiberzlochyn: teoretyko-pravovi problemy / O.O. Tykhomyrov // Zb. materialiv nauk.-prakt. konf. "Informatsiina bezpeka: vyklyky i zahrozy suchasnosti"; 5 kvitnia 2013 r. – K. : Nauk.-vyd. tsentr NA SB Ukrainy. – 2013. – S. 180.
9. Problemy chynnoi vitchyznianoi normatyvno-pravovoi bazy u sferi borotby iz kiberzlochynnistiu: osnovni napriamy reformuvannia : analitychna zapyska/ D. Dubrov, M. Ozhevan, [Electronic source]. – Access mode: http://www.niss.gov.ua/articles/454
10. Pro vyklyky ta zahrozy natsionalnii bezpetsi Ukrainy u 2011 rotsi: rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 17.11.2010 r. // Ofitsiinyi visnyk Prezydenta Ukrainy. – 2010. – № 33.
11. Pro skasuvannia deiakykh rishen Rady natsionalnoi bezpeky i oborony Ukrainy: Rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28.04.2014 r. // Ofitsiinyi visnyk Ukrainy. – 2014. – № 47.
12. Pro borotbu z teroryzmom. Zakon Ukrainy. vid 20.03.2003 № 638 IV // Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2003. – № 25.
13. Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy: analitychna dopovid [Electronic source] // Natsionalnyi instytut stratehichnykh doslidzhen. – 2011. – Access mode do resursu: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf

Дробожур Р.Р., Малишев М.А.
Національний університет «Одеська юридична академія»

НЕДОЛІКИ ТА ПРОПОЗИЦІЇ З ВДОСКОНАЛЕННЯ НОРМАТИВНО-ПРАВОВОЇ СКЛАДОВОЇ МЕХАНІЗМУ ПРОТИДІЇ ЗЛОЧИНАМ У СФЕРІ ІКТ

Анотація
Роботу присвячено аналізу українського законодавства у сфері протидії злочинам у сфері кібербезпеки а також вивченню практики правоохоронних органів у даній сфері. Ефективний механізм боротьби проти злочинності у сфері інформаційно-комунікаційних технологій (ІКТ) передбачає комплексне використання трьох підходів – інженерно-технічного, організаційного та нормативно-правового. Серед вказаних підходів основоположним і системоутворюючим є саме нормативно-правовий, механізми якого, безумовно, застосовуються комплексно разом із організаційним та інженерно-технічним напрямом і полягають у створенні законодавчих засад реалізації механізмів перших двох напрямів. Відтак, саме аналіз законодавчих основ боротьби зі злочинами у сфері ІКТ дає змогу найбільш глибоко дослідити недоліки сучасних механізмів забезпечення кібербезпеки та виявити першопричину проблем їх неефективності. В статті приведено детальний аналіз вітчизняного законодавства в інформаційний сфері загалом та у сфері забезпечення кібербезпеки зокрема, виявлено окремі його недоліки та наведено пропозицій усунення таких недоліків.
Ключові слова: кіберзлочин, кіберпростір, інформаційно-комунікаційні технології, інформаційна безпека, захист інформації.

Дробожур Р.Р., Малышев М.А.
Национальный университет «Одесская юридическая академия»

НЕДОЧЕТЫ И ПРЕДЛОЖЕНИЯ ПО УСОВЕРШЕНСТВОВАНИЮ НОРМАТИВНО-ПРАВОВОЙ СОСТАВЛЯЮЩЕЙ МЕХАНИЗМА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИКТ

Аннотация
Работа посвящена анализу украинского законодательства в сфере противодействия преступлениям в сфере кибербезопасности а также изучению практики правоохранительных органов в данной сфере. Эффективный механизм борьбы против преступности в сфере информационно-коммуникационных технологий (ИКТ) предусматривает комплексное использование трех подходов – инженерно-технического, организационного и нормативно-правового. Среди указанных подходов основополагающим и системообразующим является именно нормативно-правовой, механизмы которого, безусловно, применяются комплексно вместе с организационным и инженерно-техническим направлением и заключаются в создании законодательных основ реализации механизмов первых двух направлений. Следовательно, именно анализ законодательных основ борьбы с преступлениями в сфере ИКТ дает возможность более глубоко исследовать недостатки современных механизмов обеспечения кибербезопасности и выявить первопричину проблем их неэффективности. В статье приведен детальный анализ отечественного законодательства в информационной сфере в целом и в сфере обеспечения кибербезопасности в частности, выявлены отдельные его недостатки и приведены предложения по устранению таких недостатков.
Ключевые слова: киберпреступление, киберпространство, информационно-коммуникационные технологии, информационная безопасность, защита информации.