UDC 343.1 (477): 65.012.8 + 004
Oleksandr V. Manzhai –
candidate of juridical sciences, associate professor,
assistant professor of the
department of information security of
Kharkiv National University of Internal Affairs
(27, prosp. 50-richya SRSR, Kharkiv, Ukraine)

Organizational Features of Cybercrime Fighting in Ukraine

Стаття присвячена дослідженню організаційних особливостей боротьби з кіберзлочинністю в Україні. Проаналізовано нормативно-правову базу боротьби з кіберзлочинністю. Визначено роль та функції підрозділів боротьби з кіберзлочинністю. Проаналізовано шляхи конвергенції організованої злочинності та кіберпростору. Розглянуто інформаційне забезпечення боротьби зі злочинністю та систему підготовки фахівців для підрозділів боротьби з кіберзлочинністю. Запропоновано розробити інструкцію щодо здійснення оперативно-розшукових заходів з використанням кіберпростору.
Ключові слова: *боротьба з кіберзлочинністю, організаційні особливості, організована кіберзлочинність, підготовка фахівців, правоохоронні органи.*

Статья посвящена исследованию организационных особенностей борьбы с киберпреступностью в Украине. Проанализирована нормативно правовая база борьбы с киберпреступностью. Определены роль и функции подразделений борьбы с киберпреступностью. Проанализированы пути конвергенции организованной преступности и киберпространства. Рассмотрено информационное обеспечение борьбы с преступностью и система подготовки специалистов для подразделений борьбы с киберпреступностью. Предложено разработать инструкцию по осуществлению оперативно-розыскных мероприятий с использованием киберпространства.
Ключевые слова: *борьба с киберпреступностью, организационные особенности, организованная киберпреступность, подготовка специалистов, правоохранительные органы.*

The article deals with organizational features of cybercrime fighting in Ukraine. Laws and regulations of cybercrime fighting are analyzed. Role and functions of cybercrime units are identified. Ways of organized crime and cyberspace convergence are probed (use of cyberspace by the organized criminal groups for the purpose of carrying out typical criminal activity; use of cyberspace along with traditional environment to extend the sphere of influence organized criminal groups on new types of criminal business; use of cyberspace by the new informal criminal groups formed to carry out criminal activity via cyberspace and aimed at interfering with the work of computer technique). The information subsystems of Law Enforcement Integrated Information Retrieval System and system of training specialists in combating cybercrime in Ukraine are exposed. It has been established that today Ukraine faces the lack of comprehensive training for the specialists in fighting against cybercrime in the following areas: educational and scientific, investigative, operative, forensic activities, which particularly was emphasized by the staff of territorial branches of the Ministry of Internal Affairs. The analysis has also established that there is an urgent need to develop the procedure and practical guidelines for conducting operative and search measures via the cyberspace within law enforcement authorities of Ukraine. Implementation of the mentioned documents into practical activity will allow to remove ambiguity in this field. This step can also help to reform the system of cybercrime fighting in Ukraine.
Keywords: *cybercrime fighting, organizational features, organized cybercrime, specialists training, law enforcement authorities.*

Issue. It has been several decades since high technologies started being actively introduced into all the spheres of human activity. This process accelerates every year. When new computer technologies came out, people, who began using computers with illegal purpose, appeared almost at the same time. Before, those were people who had a wealth of knowledge and experience in high

technology, but it is not common that the computer infringement is done by ordinary citizens who have only basic computer skills. Because of the circumstances mentioned above the law enforcement agencies could not remain aloof and fight actively against cybercrime [1, p.141].

Analysis of recent research and publications. In Ukraine the cybercrime fighting was explored by such scholars as O.M. Bandurka, V. M. Butuzov, N. L. Volkova, I. O. Voronov, V. O. Golubev, O. F. Dolzhenkov, V. Y. Zhuravlyov, G. V. Zahika, V. P. Zakharov, M. Y. Litvinov, Y. Y. Orlov, M. M. Perepelytsya, E. V. Ryzhkov, L. P. Skalozub, Y. V. Stepanov, I. F. Haraberyush, V. G. Hahanovskyy, V. P. Shelomentsev and others. Different aspects of cybercrime fighting considered Russian researchers S. S. Ovchynskii, V. S. Ovchynskii, A. S. Ovchynskii, A. L. Osypenko, researchers from the U.S. Joel McNamara, Stephen Heymann, David Green, Tony Whitledge, Belorussian researcher V. E. Kozlov etc.

Unsolved problems. The system of cybercrime fighting in Ukraine nowadays is in the making. So there are certain issues in organization of such activity. Particularly issues of effective fighting against organized cybercrime remain unsolved. The publication analysis has established that considering the language barrier there is a lack of comprehensive foreign research in the field of Ukrainian system of cybercrime fighting.

So **the objective of this article** is to highlight some specific features of organization of cybercrime fighting in Ukraine.

The main body. Laws and regulations of cybercrime fighting in Ukraine consist of the Constitution of Ukraine [2] with article 17 stating that the information security of Ukraine is the vital task of the state.

Apart from the Constitution regulations concerning cybercrime fight can be found in Convention on Cybercrime dated 23.11.2001 ratified by the Verkhovna Rada of Ukraine on 07.09.2005 (hereinafter the Convention) [3]. According to the Convention rules, member states must take actions at the national level aimed at fighting against cybercrime.

Apart from the Convention on Cybercrime laws and regulations regarding cybercrime fight include provisions of the Criminal Code of Ukraine [4] and the Code of Criminal Procedure of Ukraine [5], article 263 (receiving information from transmit telecommunication networks), article 264 (receiving information from electronic information systems), article 268 (location of radio electronic device), article 274 (surreptitious obtaining of samples necessary for comparative study). A big role in cybercrime fight is played by the Law of Ukraine *On Operational-Investigative Activity* [6] and a number of other legislative acts.

Among statutory instruments the most important are the Order of the Ministry of Internal Affairs of Ukraine (MIA) *On Organizing of Work of the Cybercrime Division of the MIA of Ukraine and Cybercrime Units of Chief Division of the Ministry of Internal Affairs of Ukraine* [7] and a number of departmental orders and instructions aimed at cybercrime fighting.

Cybercrime counteraction in the system of the Ministry of Internal Affairs of Ukraine is the prerogative of the cybercrime units that are a part of the Cybercrime Division of the MIA of Ukraine (fig. 1).

Fig. 1.The Cybercrime Division of the MIA of Ukraine

Cybercrime units take part in formation and implementation of state policy aimed at prevention of crimes and offences that involve computers, computer systems and computer or telecommunications networks when planned, committed or concealed; as well as crimes and offences committed by means of computers (cybercrime area) (fig. 2).

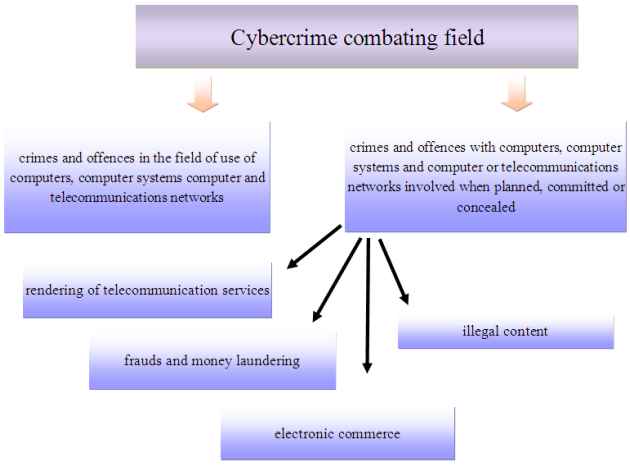

Fig. 2. Cybercrime combating field

Core **functions** of the cybercrime units are as follows:

- defining, development and taking organizational and practical measures aimed at prevention and counteraction to crimes and offences related to cybercrime units;
- finding out the courses and conditions which cause crimes and offences that come under the jurisdiction of cybercrime units;
- taking measures to eliminate them;
- according to the legislation carrying out the special investigative activity in the field of telecommunication and Internet services, financial establishment and cash register systems in order to receive information which will contribute to detection of crimes under the jurisdiction of cybercrime units;
- indicating guidelines and tactics of the special investigative activity in the field of cybercrime fighting;
- carrying out special investigative activity as stated in the legislation and other statutory instruments;
- taking measures of prevention, detection and investigation of crimes within the cybercrime units activity area under and in accordance with the legislation;
- according to the legislation and with the purpose of meeting the requirements of special investigative activity to create and update information databases;
- organizational and operational support of criminal investigations, brought by cybercrime units;
- short- and long-term planning of the work and effectiveness improvement measures;
- with the consent of the Ministry of Internal Affairs headquarters holding complex and target-oriented crime-prevention activities, involving foreign law enforcement agencies;
- making proposals under the established procedure as to the improvement of the regulatory system in the field of cybercrime combating;
- participation in the international contract drafting related to cybercrime counteraction within their competence. Study and use of positive domestic and foreign experience of cybercrime combating.
- collection, summarizing, systematization and analyses of the information about the criminal situation and crime counteraction within the cybercrime combating units priority area at the national regional levels. Reporting according to the legislation the results of work and relevant information to the Ministry, the State government bodies, educational institutions, enterprises, establishments and organizations dealing with counteraction to crimes and offences under the jurisdiction of cybercrime units.

We should also note, that establishment of Cybercrime Division made a significant positive effect. Lately, the media increasingly gives the reports about detectives of Cybercrime Division, performing successful operations to stop the criminal activities of organized crime groups on the Internet, and both traditional types of crime with the use of cyberspace and the so-called cybercrimes [1, p. 145].

There are three ways of organized crime and cyberspace convergence in Ukraine and abroad nowadays. They are as follows:

- **use of cyberspace by the organized criminal groups for the purpose of typical criminal activity**. Cyberspace can be used by drug dealers or terrorist centers as a telecommunication networks to exchange codified messages or to blackmail or to contact victims.

For example in 2012 mass media spread the information about extortion of money on behalf of the Security Service of Ukraine. Operating system is blocked by a virus and money is needed to restore it. The number of a bank electronic purse is given and the amount of 2 thousand hryvnias is requested. Most of such schemes were detected in Ivano-Frankivsk region [8].

Cyberspace is often used by organized criminal groups which are engaged in espionage and counter-espionage. In China, for example, drug dealers tried to prevent their detection by penetrating

into the custom database in order to change the information about the consignment. Colombian and Mexican drug cartels use modern equipment to watch the employees who conduct investigations and eavesdropping, to make photographs and gather personal information. Criminals stole personal computer and disks that belonged to investigatory powers [9]. Later, the information from these disks was used to eavesdrop police officers and to have them under surveillance. Criminal groups have recently spread false information via the Internet to receive speculative gains, to discredit law enforcement or trample competitors [10]. Porno-peddling is another activity carried out by organized criminal groups;

- **use of cyberspace along with traditional environment to extend the sphere of influence of organized criminal groups on new types of criminal business.** They are, as a rule, the following: counterfeit products, bank thefts via electronic networks, cracking of credit card data bases etc.

- **use of cyberspace by the new informal criminal groups established to carry out criminal activity via cyberspace and aimed at interfering with the work of computer technique.** These groups are not subordinated to organized criminal groups in the usual sense. The examples of such groups are groups of hackers.

Among the above mentioned the latter activity carried out by organized crime in cyberspace is rather new and the least investigated by the Ukrainian law enforcement. One of the characteristic features of such informal groups is the absence of direct contact of its members as well as its transnational nature. They do not have leaders; group members do not know each other personally; their activity is coordinated via network technologies. Groups emerge as temporal unions to complete certain tasks and are characterized by a high level of inconstancy (after the task has been completed groups can break up or be rearranged) [11, p. 43].

Such groups are also characterized by high professional level of crimes committed through cyberspace as well as effective concealment of traces. All these factors complicate the process of detection, investigation and prevention of such crimes [12, p. 260-262].

Electronic records play an important role in the cybercrime fighting in Ukraine. The Law Enforcement Integrated Information Retrieval System consists of the following information subsystems:

1. **"Fact"** – information about events, crimes, law violations, accidents, stated in applications (messages, reports) registered in the call center of a local law enforcement body; crimes committed or prepared; administrative offences; incidents which threaten to personal or community safety; non-criminal events, including accidents, fires, catastrophes, natural disasters and other emergency events.
2. **"Crime"** – information about the registered undetected crimes, committed in the area of responsibility of a law enforcement body, including those which resulted in instituting a case in the "Crime" category in compliance with the law requirements, which regulate organization of investigative and search activities in law enforcement bodies.
3. **"Bringing to a police station"** – persons brought to a law enforcement body.
4. **"Individuals"** – information about the persons who committed offences and with whom preventive work is performed by law enforcement personnel.
5. **"Wanted"** – information about the persons who hide from pre-trial investigative bodies or trial, escape from serving the sentence, as well as missed people.
6. **"Identification" –** information about missed people, establishing identity of unidentified dead bodies.
7. **"Thing"** – information about the things which were stolen, seized as forged, prohibited or having limited circulation from persons, ownerless things which were found or seized from cloak rooms at railway stations, ports, airports, and were taken to a law enforcement body.

7.1. **Workbench "Numbered things"** – things which have individual manufacture numbers.

7.2. **Workbench "Antiques"** – cultural values – objects of material and spiritual culture, which have artistic, historic, ethnographic and scientific importance.

8. **"Stolen cars"** – information about the vehicles being searched and vehicles without owners as well as stolen and lost vehicle state registration number plates.
9. **"Lost documents"** – information about documents (document forms), which were stolen, lost, seized as forged from persons, passports

of deceased citizens of Ukraine, which were not handed over to law enforcement bodies, passports of wanted people, documents which have individual manufacture numbers and are in state circulation.

10. **"Criminal weapons"** – information about the weapons, which were stolen, lost, found, handed over to law enforcement bodies, seized by law enforcement personnel as kept illegally, irrespective of its technical condition, which have individual manufacture numbers or numbers of parts.

11. **"Registered weapons"** – information about the weapons, which have individual manufacture numbers and are in use of citizens, enterprises, institutions, organizations, economic amalgamations, who are legally authorized to acquire, keep, carry, and transport weapons which are registered by units of law enforcement weapon registration system.

12. **"Administrative offences"** – information about the administrative offences registered in law enforcement bodies which resulted in administrative offence reports drawn up by the authorized law enforcement personnel.

13. **"Electronic report"** – information which was obtained by law enforcement officers while performing their duty or during open search from citizens or officials (without disclosing the information source and only of open nature).

14. **"Migrant"** – information about the individuals who violated the Ukrainian law on legal status of foreigners, stateless persons, who were found by law enforcement personnel.

15. **"Corruption"** – information about the registered criminal and administrative corruption offences and the persons who committed them.

Nowadays Ukraine faces the lack of comprehensive training for the specialists in fighting against cybercrime in the following areas: educational and scientific, investigative, operative, forensic activities, which particularly has been emphasized by the staff of territorial branches of the Ministry of Internal Affairs.

The Order of the Ministry of Internal Affairs of Ukraine *On the Organization of Training at Kharkiv National University of Internal Affairs* dated 20.11.2012 No. 1062 established the Faculty of Training Specialists in Combating Cybercrime and Human Trafficking at Kharkiv National University of Internal Affairs.

The Faculty offers training in the following areas: "Systems of Technical Information Security", "Law" ("Cybercrime Fighting" and "Combating Trafficking in Human Beings" specializations). Thus, training in fighting against cybercrime and related areas has been concentrated at one university which provides an adequate technical components during training and is supported by the technical experts in the relevant fields (fig. 3).

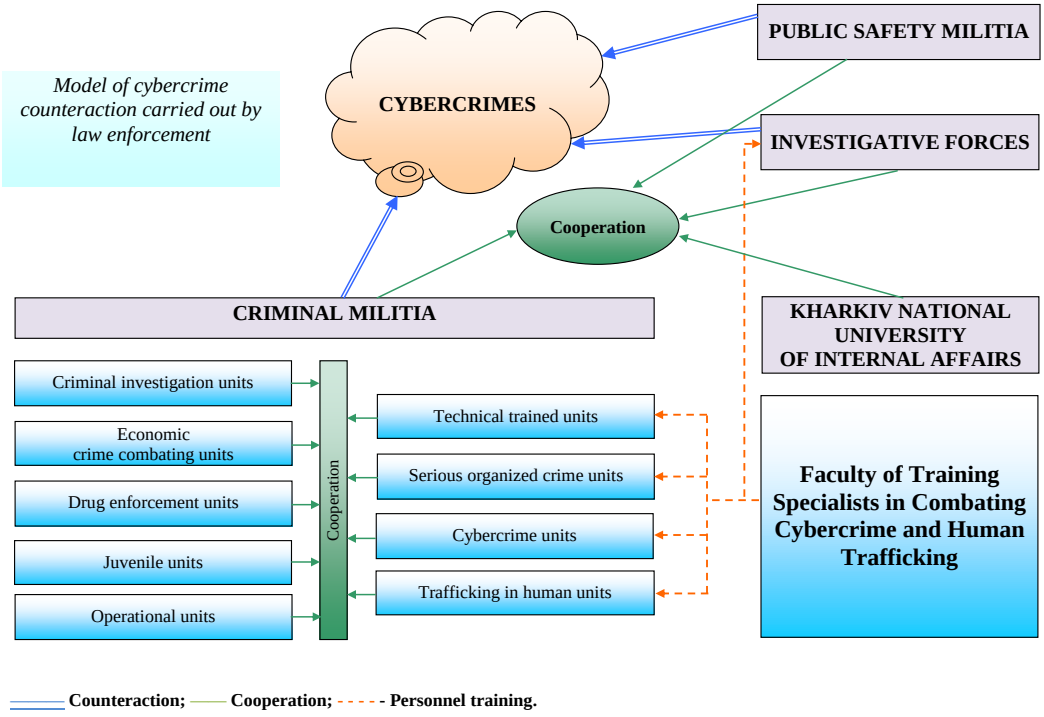

Fig. 4. Cybercrime counteraction system

Additionally as a part of the Faculty's operations, the Training Center for Combating Cybercrime and Monitoring Cyberspace has been established (on the voluntary basis) [13].

Conclusions. The analysis has established that there is an urgent need to develop the procedure and practical guidelines for conducting operative and search measures via the cyberspace within law enforcement authorities of Ukraine. Implementation of the mentioned documents into practical activity will allow to remove ambiguity in this field. This step can also help to reform the system of cybercrime fighting in Ukraine.

References

1. O. V. Manzhai Procedure for Analyzing Special Investigative Actions through Cyberspace in Countries of Common and Continental Law / O. V. Manzhai // Vnutrishnia bezpeka (Internal Security). – 2012. – No. 1 (4). – P. 141-152.

2. The Constitution of Ukraine // Vidomosti Verkhovnoi Rady Ukrainy (VVR) (the Official Bulletin of the Verkhovna Rada of Ukraine). – 1996. – No. 30. – Art. 141.

3. On Cybercrimes : Council of Europe Convention: dated 07.09.2005 [Online resource]. – Access : http://zakon4.rada.gov.ua/laws/show/994_575.

4. The Criminal Code of Ukraine : dated 05.04.2001 [Online resource]. – Access : http://zakon.rada.gov.ua/go/2341-14.

5. The Code of Criminal Procedure of Ukraine : dated 13.04.2012. [Online resource]. – Access : http://zakon2.rada.gov.ua/laws/show/4651-17.

6. On Operational and Search Activity : the Law of Ukraine dated 18.02.1992. [Online resource]. – Access : http://zakon.rada.gov.ua/go/2135-12.

7. On Organization of Work of the Cybercrime Division of the MIA of Ukraine and Cybercrime Units of Chief Division of the Ministry of Internal Affairs of Ukraine : Order of the Ministry of Internal Affairs of Ukraine dated 30.10.2012 No. 988 [Online resource]. – Access : http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc130740.html.

8. SSU Searches for Internet-Racketeers [Online resource]. – Access : http://podrobnosti.ua/podrobnosti/2012/02/13/820044.html.

9. A. I. Gurov, Modern Technologies in Drug Business / A. I. Gurov, T.M. Vinogradskaia, B. F. Kalachiov [Online resource]. – Access : http://www.narkotiki.ru/mir_5553.html.

10. A. V. Kuznetsov, Report at the VII International Conference "Law and the Internet" / A. V. Kuznetsov [Online resource]. – Access : http://www.securitylab.ru/opinion/241966.php.

11. A. L. Osypenko, About Some Features of Clearing of Network Computer Crimes / A. L. Osypenko // Nauchnii Portal MVD Rossii (The Scientific Portal of the MIA of Russia). – 2010. – No 2 (10). – P. 42-47.

12. O. M. Bandurka, Special Investigation Activity Comparative Studies / O. M. Bandurka, M. M. Perepelytsia,O. V. Manzhai and V. V. Shendrik. – Kharkiv : Zolota Milyia, 2013. – 352 p.

13. About the Cybercrime Combating and Cyberspace Monitoring Training Center (on the Voluntary Basis) [Online resource]. – Access : http://cybercop.in.ua/index.php/en/about-the-center.