UDC 343.1

INVESTIGATION OF NEW FORMS OF CYBER CRIME (PHISHING AND CYBERSQUATTING)

РОЗСЛІДУВАННЯ НОВИХ ФОРМ КІБЕРЗЛОЧИННОСТІ (ФІШИНГУ ТА КІБЕРСКВОТІНГУ)

Yatsyk T.P.,
Candidate of Juridical Sciences (Ph.D.),
Associate Professor of Department of Criminal Process and Criminalistics
of the University of the State Fiscal Service of Ukraine

Shkelebei V.A.,
Candidate of Juridical Sciences (Ph.D.),
Senior Teacher of Department of Criminal and Criminal Procedural Law
of the National University "Kyiv-Mohyla Academy"

In article new types of crimes which are committed in information space (virtual space) are considered. The international practice in fight against these crimes is analyzed. Problems and the directions of enhancement of effective fight against phishing and cybersquatting are determined.
Key words: information space, virtual space, cyber-terrorism, phishing, cyber-attacks, cybersquatting.

У статті розглядаються нові види злочинів, які вчиняються в інформаційному (віртуальному) просторі. Аналізується міжнародна практика у боротьбі з цими злочинами. Окреслюються проблеми та напрями вдосконалення ефективної боротьби з фішингом та кібер-сквотингом.
Ключові слова: інформаційний простір, віртуальний простір, кібертероризм, фішинг, кібер-атаки, кібер-сквотинг.

В статье рассматриваются новые виды преступлений, совершаемых в информационном (виртуальном) пространстве. Анализируется международная практика в борьбе с данными преступлениями. Определяются проблемы и направления совершенствования эффективной борьбы с фишингом и кибер-сквоттингом.
Ключевые слова: информационное пространство, виртуальное пространство, кибертерроризм, фишинг, кибер-атаки, кибер-сквотинг.

Distribution of new information technologies which cornerstone wide use of the computer equipment and means of communications, optimization and automation of processes in all spheres of activity has led together with it to leveling of borders and an interlacing of national economies and national infrastructures of the countries of the world.

Such tendencies have led to formation of uniform world information space where everyone can get access to any information in an every spot on the globe, exercise remotely controls of own assets and assets of the company, to sign economic contracts with foreign subjects of managing without the need for personal contact, etc.

At the same time, information space became the place and at the same time the instrument of crime. From now on crime doesn't demand preliminary «processing of the client» and personal contact with the potential victim. The computer and access to information and communication systems where he by means of computer viruses and other illegal technical means gets access to databases, bank accounts, automated control systems becomes the main tool of the criminal only [1].

Rapid growth of the number of the crimes committed in a cyberspace in proportion to number of users of computer networks (by estimates of the Interpol, growth rates of crime on the global Internet, are the fastest on the planet). It once again emphasizes a condition of danger from information and cyber-terrorism [2, p. 112].

Separate aspects of development and formation of information relations, questions of implementation of counteraction of cybercrime were considered by the leading domestic scientists as: N.A. Budakov, V.M. Butuzov, N.N. Galamby, R.A. Kalyuzhny, V.V. Kovalenko, Ya.Yu. Kondratyev, B.A. Kormich, Yu.E. Maksimenko, A.I. Marushchak, V. Novitsky and foreign experts A. Robert, K. Osakva, T. Blentan, D. Banisar, etc. However need of further scientific search is proved by existence of gaps in the national legislation on a regulation of counteraction of cybercrime in Ukraine and lack of a legal regulation of conducting investigation of these crimes.

Purpose of scientific research – it to open the mechanism of investigation and to characterize a circle of subjects of investigation of cyber-crimes (a phishing and a cyber-skvoting).

Statement of the main material. The term «cyber-terrorism» has been entered by J. Collin in the mid-eighties. Subsequently M. Pollit has offered the following definition of cyber-terrorism: "deliberate, politically motivated the attack against information, computer systems, computer programs and databases in the form of unauthorized invasion from the international groups or secret agents".

According to the European Convention 2001 from cyber-crimes, means of cyber-terrorism: computer system, computer data, services ICT and data of traffic.

Cyber-terrorism – deliberate, politically motivated attack to information which is protected by the law, in

critical segments of the state and also in the private sector, presented in electronic form on machine carriers, by means of criminal use of an information system, creating danger of death of people, causing's significant property damage, causing other socially dangerous consequences or threat of commission of the specified actions on purpose, inherent in terrorism.

Cyber-terrorism is now very serious problem which it is impossible to leave unnoticed and to neglect threats which it causes.

The relevance of fight and investigation of cyber-crimes will grow in process of development and distribution of information and telecommunication technologies.

According to the American experts, the most vulnerable points of infrastructure is the power, telecommunications, aviation dispatching offices, financial electronic and government information systems and also automated control systems for troops and weapon [3, p. 57].

Every day computer systems are exposed to the attacks of hackers and it causes negative consequences for users. However the biggest problem is the hacker attacks to computers of large corporations and public authorities of management. Such actions of cyber-criminals is threat not only functionality of some enterprise or public authority, but also national economy in general.

According to the analysis which is carried out by the "FireEye" company in the countries of the Middle East, Europe and Africa all the government websites, the websites of the financial organizations and the websites of telecom operators suffer from cyber-attacks [4].

Spread of computer viruses, frauds with plastic payment cards, thefts of funds from bank accounts, plunder of computer information and violation of the rules of operation of the automated electronic computing systems is not a full list of similar crimes. This category of crimes is called differently: cyber-crimes, computer crimes, crimes in the sphere of computer technologies, crimes in the sphere of computer information.

Now in domestic criminalistics still there is no accurate definition of a concept of cyber-crime and data and uniform staly classification of crimes which unite a concept of cyber-crime is unavailable. For today there are two main directions of a scientific thought. One part of researchers carries to action cyber-crimes in which the computer is an object or means of encroachment. Researchers of other group refer only illegal actions to cyber-crimes in the sphere of automatic information processing. That is subject to encroachment is information processed in computer system, and means of commission of crime is the computer.

The criminalistics feature of cyber-crimes is that investigation and disclosure of these crimes is impossible without application and use of computer technologies. It is connected with need of search, fixation, withdrawal and collecting proofs for an electronic form. Also computer technologies are widely used for conducting investigation and search operations.

In the Swiss city of Davos from January 25 to January 29, 2012 there took place the 42nd World Economic Forum. During a forum the speech was made by the director of the European police office (Europol) Rob Uaynrayt who has focused attention of participants of a forum on cybercrime threat. During the speech the director of Europol in particular has pointed that personal data is new goods which are offered by cybercrime. During an era of digital technologies of people it is easy to identify through figures (bank accounts, passwords, etc.). These figures became the main subject of trade for swindlers around the world.

Within these research cyber-crimes as a result of which there is financial or other material benefit in the form of illegally gained income are most in detail considered. First of all, it is about use of information and communication systems and computer technologies for access to a private property of persons and further actions for management or the order of this property.

Our state is promptly reconstructed on the European standards of management today, there is a modernization of all branches of the state, but along with new progressive opportunities new types of crimes appear. So, for example, with transition of the state to non-cash currency new forms of cyber-crimes have appeared: phishing [5].

Phishing the attack is an attempt to obtain your personal information on the Internet in the deceptive way.

The phishing attacks are usually carried out through the e-mails, announcements or the sites similar to those which you visit. For example, you can receive the e-mail, similar on the letter from bank with a request to confirm the bank account number.

The phishing (on English Phishing, comes from fishing – fishing, production) is the most popular method in Internet space which is used for breaking of passwords and theft of confidential information. For example: payment data of the credit card, bank user names and passwords, data from personal pages of the user, access to bank accounts, financial information etc. [4].

For the purpose of taking by information swindlers go for various tricks: carry out mass mailing of e-mails (spam) and also personalized messages from financial and public institutions, social networks, create the phishing websites, loading pages, pop-up windows, etc.

Fundamental element of a phishing or the phishing attack is process of creation of the duplicating copy or a clone of the known website for the purpose of theft of the password of the user or other protected information. This method has received great popularity as most of users aren't always observed elementary requirements of computer safety.

Using various psychological receptions, phishing swindlers induce users to enter the confidential data on the false web page (phishing website) externally not different from the original website taken by swindlers as a basis for copying.

As a result of such actions, the user gets on the page of a phishing, practically without distinguishing from the original, and enters the confidential information. In the same second she becomes famous to swindlers and can be used for further illegal actions [5].

Electronic business is included more and more in high gear into our life, influencing our behavior, chang-

ing our preferences. He is in a condition of dynamic development now, more and more additions and network decisions by means of which even more often business activity in traditional segments of economy adapts to requirements of «new economy» and is in whole or in part transferred to cybernetic space are created.

Traditionally, we perceive electronic business in the form of trade in goods on the Internet. But, it is not all scopes of electronic business. E-business it is also electronic auctions, electronic reference books, casino, remote education and e-mail and also such unusual type of business as a cyber-skvoting.

Kiber-skvoting – the phenomenon which consists in registration of a domain name is identical with commercial designation of other person (often well-known legal / natural person) for the purpose of receiving profit (to sell a domain name, to interfere with activity of the competitor, to receive more «clicks» owing to emergence of associations with a certain person) [6, p. 48].

The most widespread types of modern cyber-skvoting are: 1) a branch cyber-skvoting – registration of domains according to the name of kinds of activity, goods, services and so forth; 2) a branded cyber-skvoting – registration of the domain names containing popular trademarks, trade names, that is means of individualization protected by the law; 3) a personalized cyber-skvoting – registration of the domains coinciding with surnames of the famous people; 4) a geographical cyber-skvoting – registration of domain names in the form of place names (names of the city, area, country, island, etc.); 5) a protective cyber-skvoting – registration by the legal owner of the popular website (trademark) of domain names of relatives, conformable, similar, connected on sense with his own domain name; 6) The Tayp-skvoting – registration of the domain names close on writing to addresses of the popular websites counting on a mistake of users [7].

In Ukraine exists Cyberpolice which task has to be an ensuring cyber security of the country and prevention of cybercrime. But there is no uniform base of key terms and concepts aren't developed the criminalistics equipment and tactics, using which the staff of Cyberpolice could make investigations of cyber-crimes effectively.

The SSU and the Ministry of Internal Affairs represented by Management on fight against cybercrime have appeared at peak of war with "cybers". Unfortunately, their effort isn't enough. Especially, considering our Ukrainian realities. If earlier the Ukrainian programmers hackers wrote programs viruses for breaking and data theft in the rich western countries, then now in connection with strengthening of fight of the American and European power against computer crimes their attention was paid also to Ukraine.

Our country with her low level of awareness on threats of use of computers and the low level of information security becomes for them the real Klondike. Embezzlement in the systems of Internet banking, these credit cards, fraud in information networks and insider information leakages become the daily phenomena.

So, according to the experts Managements on fight against cybercrime only for the last months in Kiev about twenty cases of theft of money through the client bank are fixed. The sums are from 20 thousand to 40 million UAH. However the similar facts are hushed up, there are practically no messages in media about them. Neither the victim, nor banks, nor militia not favorable noise around what occurs. Often there are situations when such roguish schemes are implemented by organized groups into which representatives of banks and law enforcement agencies enter [8].

It should be noted that rapid development of the sphere of information technologies constantly generates new types of service, including in the financial sphere. It, in turn, forces criminals to improve the abilities and to think out new ways of illegal earnings in a cyberspace.

To overcome, to brake development of cybercrime it is necessary to make at the national level the strategy for fight against this type of crimes containing concrete measures of effective fight and prevention which would be directed to decrease in risk of commission of crimes and neutralization of potentially harmful consequences for individuals and society more precisely.

Adoption of laws, the strategy of counteraction of cybercrime, effective management, development of capacity of bodies of criminal justice and law enforcement agencies, information and educational activity, creation of the strong knowledge base and cooperation between state bodies, communities, the private sector and the international organizations belong to number of optimum measures in the field of prevention and effective investigation of cybercrime.

REFERENCES:

1. Кіберзлочинність та відмивання коштів. URL: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf.

2. Яцик Т.П. Розслідування інформаційного тероризму та кібер-тероризму (міжнародно-правовий аспект). Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). Вип. 1 (5) 2017. С. 111−115.

3. Ліпкан В.А. Інформаційна безпека України: [глосарій] / В.А. Ліпкан, Л.С. Харченко,О.В. Логінов. К.: Текст, 2004. 136 с.

4. Regional advanced threat report Europe, Middle East and Africa 2014. URL: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-emea-advanced-threat-report-1h2014.pdf.

5. Что такое фишинг, общее представление и примеры. URL: https://hetmanrecovery.com/ru/recovery_news/what-is-phishing-overview-and-examples.htm.

6. Ходаківський Є.І. Інтелектуальна власність: економіко-правові аспекти: навчальний посібник / Є.І. Ходаківський, В.П. Якобчук, І.Л. Литвинчук. К.: «Центр учбової літератури», 2014. 276 с.

7. Киберсквотинг: украинские особенности. Часть первая. URL: http://cybersquatter.com.ua/?p=53.

8. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. Економічна правда. 2013. 26 лютого. URL: https://www.epravda.com.ua/news/2013/02/7/360508/.