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. Оокреслюються проблеми та напрями вдосконалення ефективної боротьби з фішингом та кібер-сквотингом.

Ключові слова: інформаційний простір, віртуальний простір, кібертероризм, фішинг, кібер-атаки, кібер-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 systems, computer programs and databases in the form of unauthorized invasion from the international groups or secret agents”.

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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes 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 stable 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 crimes of cyber-criminals is threat not only functionality of some enterprise or public authority, but also national economy in general.
інших наших підходів. Він є у вигляді динамічного розвитку, наскільки він додаткові і віднесені колоній до витоків нової економічної моделі й відповідно до нього зібрано в сегментах економічної кооперації. Буде створено у вітчизняних умовах.

Традиційно, ми клали електронну торговлю в формі бізнесу його основних підприємств, а також у вигляді казино, лотерей, електронних аукціонів, електронних бібліотек, онлайн-казино, і так далі. Електронна торгівля - це також форма роботи з товаром на інтернеті. Проте, вона не є формою cyber-squating.

Kiber-skvoting – явище, що складається з реєстрації домену, яке відповідає назві виду діяльності, продукції, послуг і так далі; 2) брендування cyber-squating – реєстрація доменів, що відповідають популярним брендам, торгівлі, що є результатом індивідуалізації, заохочує закон; 3) географічний cyber-squating – реєстрація доменів з назвами місць проживання знаменитих людей; 4) географічний cyber-squating – реєстрація гарячих доменів, що відповідають назвам місць проживання таких людей; 5) просторовий cyber-squating – реєстрація доменів, що відповідають назвам відповідного рівня, співвідношення і чистоти, залежать від спеціалізованої діяльності на основі свого доменного імені; 6) The Tapp-skvoting – реєстрація доменів, що відповідають назвам відповідного рівня, співвідношення і чистоти, залежать від спеціалізованої діяльності на основі свого доменного імені. Как и в случае с кибер-пиратами, требуется разработка новых методов получения дохода в сете.

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: