ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.39 Nº 68
Enero
Junio
2021

Cuestiones Políticas Vol. 39, Nº 68 (Enero - Junio) 2021, 844-865
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Modern methods of computer-related fraud: legal characteristics and qualification

DOI: https://doi.org/10.46398/cuestpol.3968.55

Olga Kryshevych *
Igor Andrushchenko **
Olexandr Striltsiv ***
Yuriy Pyvovar ****
Olena Rivchachenko *****

Abstract

Due to the spread of new methods of committing fraudulent actions using electronic devices, the problem arose to provide you with adequate characteristics of criminal law for the development of measures leading to counteracting such crimes. The objective of the article was to identify common methods in Ukraine of committing fraud using computers, to assess the characteristics of criminal law that these crimes have, and, in turn, to determine measures to counter them. Methodologically, this is a documentary investigation. The scientific novelty of the study's findings was to identify methods of performing fraudulent actions using electronic computers that will improve the legal qualification of crimes and affect the prosecution of persons guilty of committing such illegal actions. Measures to prevent such criminal offences were also developed. The results of the study help improve the work of law enforcement agencies in Ukraine, in determining recurrent methods of committing fraudulent actions using electronic means and their proper qualification, providing an opportunity to prosecute those who commit such illegal actions and develop ways for cybercrime research and prevention in general.

* PhD in Law, Associate Professor, National Academy of Internal Affairs, Professor of the Criminal Law Department, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-6136-8106. Email: kryshevycholga@i.ua

** PhD in Law, Associate Professor, National Academy of Internal Affairs, Economic Security and Financial Investigations Department, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-2988-7579. Email: andrushchenko2000@i.ua

*** PhD in Law, Senior Researcher, Anti-Corruption Commissioner, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-8324-3053. Email: striltsivolexandr@i.ua

**** PhD in Law, Professor, National Aviation University, Head of the Constitutional and Administrative Law Department, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0001-8258-7930. Email: pyvovary@gmail.com

***** PhD in Law, National Academy of Internal Affairs, Senior Instructor of the Juridical Psychology Department, Kyiv, Ukraine. ORCID ID: https://orcid.org/0000-0002-1817-4223. Email: rivchachenkoolena@i.ua

Recibido el 15/09/2020 Aceptado el 26/12/2020

Keywords: electronic fraud; cybercrime; abuse of trust; legal qualification; criminal law in Ukraine.

Métodos modernos de fraude relacionado con la informática: características jurídicas y cualificación

Resumen

Debido a la propagación de nuevos métodos de cometer acciones fraudulentas utilizando dispositivos electrónicos, surgió el problema de proporcionarle características adecuadas del derecho penal para el desarrollo de medidas conducentes a contrarrestar este tipo de delitos. El objetivo del artículo fue determinar los métodos comunes en Ucrania de cometer fraude utilizando computadoras, valorar las características del derecho penal que tienen estos delitos y, a su vez, determinar las medidas para contrarrestarlos. En lo metodológico se trata de una investigación documental. La novedad científica de las conclusiones del estudio fue determinar los métodos de realización de acciones fraudulentas utilizando ordenadores electrónicos que mejorarán la cualificación jurídica de los delitos y afectarán al enjuiciamiento de las personas culpables de cometer tales acciones ilegales. También se desarrollaron las medidas de prevención de tales infracciones penales. Los resultados del estudio ayudan a mejorar el trabajo de los organismos encargados de hacer cumplir la ley en Ucrania, en la determinación de los métodos recurrentes de cometer acciones fraudulentas utilizando medios electrónicos y su cualificación adecuada, lo que proporciona la oportunidad de procesar a aquellas personas que cometen tales acciones ilegales y desarrollar formas para la investigación y prevención de la ciberdelincuencia en general.

Palabras clave: fraude electrónico; delito informático; abuso de confianza; calificación legal; derecho penal en Ucrania.

Introduction

The forecasts for further dependence of the vital functions of the Ukraine's infrastructure on the processes of its involvement into computerized environment and its entry into the unified information space are quite realistic. Modern society is an information technologies-oriented society based on the daily use of computers, communication networks, mobile means of communication and other technical means. Yet the information space has become a place and at the same time a direct instrument of criminal offences, as it does not require personal

contact with a potential victim, and the main tool of the offender is only a computer and access to information and communication systems, where he/she gets access to databases, bank accounts or automated management systems with the help of illegal technical means. Thus, the development of information technologies, increasing production of technical means and the scope of computer technology have given rise to new types of socially dangerous actions in which computer information is illegally used or it itself becomes the object of encroachment, the application of criminal law in the field of fighting cybercrime in general and certain criminal offences, namely computer-related fraud, the Internet. Thus, today there is a problem of providing criminal law characteristics for the reported new ways of computer-related fraud in Ukraine, which indicates the importance of this article.

1. The literature review and research methods

Scientific debates on fraud committed with the use of electronic computers indicate the peculiarity of the disposition of Part 3 of Article 190 of the Criminal Code of Ukraine (2001). One of the first attempts to provide criminal characteristics of computer-related fraud in Ukraine were suggested by Muzyka and Azarov (2005) in the textbook "Legislation of Ukraine on Criminal Liability for "Computer" Crimes: Scientific and Practical Commentary and Ways to Improving" and later on by Azarov (2007) in the book "Crimes in the Field of Computer Information (criminal law research)". At the same time, the author only outlined the general issues of criminal law characteristics of such types of fraud.

Revealing the features of legal characteristics of crimes against property committed with the use of computer technology, M. Karchevsky (2012) focuses on only one type of fraud committed with the use of electronic computers, namely via special Internet resources, designed for posting retail information either of goods or services (online auctions, online stores, etc.).

A. Vasyliev and D. Pashnev (2013) in their article "Characteristics of the Qualification of Crimes in Computerized Environment, Computer Systems and Networks and Telecommunication Networks" revealed only some features of certain types of fraud committed via information and telecommunication systems, and cases in which additional criminal law characteristics for such crimes are required. However, they did not take into account the new methods of fraud committed with the use of electronic computing. A similar thorough study is that of Dudorov (2014), in which he also revealed only the problems of qualification of fraud committed via information and telecommunication systems.

In turn, Shapochka (2015) in the article "On the Concept of Fraud Committed through the Use of Computer Networks (Cyber fraud)" reveals only the concept of cyber fraud, without providing criminal law characteristics of this phenomenon. Shevchenko and Shulyak (2018) studied the problem of putting apart computer-related fraud from other types of crimes.

Taking into account the specifics of the topic, purpose and objectives of the article, a comparative legal method was applied, which allowed to analyze the criminal law of the United States, Great Britain, France, Germany, the Kingdom of the Netherlands, the Republic of Belarus in part of criminal liability for computer-related property offences and also most common methods of commission of such criminal offences in the above-mentioned countries. The method of system analysis provided an opportunity to analyze the methods of computer-related fraud researched in scientific publications, which allowed us to summarize their elements. The use of formal-logical and system-structural methods allowed us to generalize certain methods of fraud committed with the use of electronic computers and provide for their criminal law characteristics. Basing on simulation, preventive measures as to these types of fraud were determined.

To verify the scientific provisions suggested by the researchers, we conducted a survey based on questionnaire and further interview of 30 employees of the Department of Cyber police of the National Police of Ukraine, who are directly involved in the investigation of computer-related fraud.

The survey was conducted among respondents from different regions who studied at the National Academy of Internal Affairs (Ukraine) on the basis of pre-compiled questionnaire. The questionnaire included questions about the methods of committing fraud using electronic computers already known to the authors of the article and gave the opportunity for law enforcement officers to inform about the most common in Ukraine, in their opinion, new types of these criminal offences, problems that arise during the investigation of such offences and suggest measures to counter them. In particular, during the survey, respondents noted that today the number of new types of fraud using electronic computers is growing significantly. As a result, during the criminal proceedings, problematic issues regarding the proper qualification of such new types of fraud arise. Respondents focused on the problem of defining the concept of electronic computing, because modern technologies in manufacturing new types of smartphones are blurring the difference between them and computers, which affects the criminal law characteristics of certain types of crimes and helped determine the directions for combating these offences.

2. The purpose of the article

The purpose of the article is to determine the criminal aspects of fraud committed with the use of electronic computers to further improving the law enforcement in combating this criminal offence. To achieve this goal, the following tasks were formulated:

- to analyze the existing in Ukraine and foreign countries methods of committing fraud with the use of electronic computers.
- to provide the existing methods of fraud committed with the use of electronic computers with criminal law characteristics.
- to suggest the means of responding to new threats of cybercrime and develop ways to implement them.

3. Object and subject of the research

The object of the study is public relations that arise during the detection and investigation of computer-related fraud in Ukraine, as provided for in Part 3 of Article 190 of the Criminal Code of Ukraine "Fraud". The subject of the study is to provide, on the basis of analysis of existing regulations and the results of a survey based on questionnaire of specialists involved from the Department of Cyber police of the National Police of Ukraine about the methods of computer-related fraud, their criminal characteristics and outline directions for combating such types of criminal offences.

4. Results and discussion:

4.1 The concept of cyber fraud

The popularity of the Internet is quite natural, as the user has the opportunity: round-the-clock access to a significant amount of information; fast exchange of information with other users; conducting banking, trading, stock exchange transactions from wherever you are at a convenient time and much more. What exactly is the global computer information network the Internet? It is a system of computers that are interconnected using TCP/IP protocols and have unique identification numbers (domain names). The Internet is a perfect tool in the hands of fraudsters due to the huge audience of users and the opportunity to remain anonymous. The concept of cyber fraud is covered by Part 3 of Article 190 of the Criminal Code of Ukraine (Azarov, *et al.,* 2018), according to which it is a large-scale fraud or fraud committed via illegal transactions using electronic computers.

Fraud committed through illegal transactions using electronic computers occurs when such an operation is a means of committing such criminal

offence as a result of vishing (telephone fraud with the intent of luring bank card details and transferring funds to the cards of fraudsters, for example, by calling on behalf of mobile operator to ask citizens for personal data for the unauthorized issuance of duplicate SIM cards). And having obtained the information, fraudsters issued quick loans on these bank details and misappropriated the money from the accounts of Ukrainians, and as a result of phishing (luring of confidential data - passwords, bank card numbers, PIN-codes), fraud with ATMs: data compromising (skimming and ICS-dropping), cash trapping.

Agreeing with V. Finageev (2016) we would like to note that the methods of committing criminal offences can be differentiated into three main groups: 1) methods of illegal access to bank accounts, related to the payments by payment orders; 2) methods of committing criminal offences related to illegal access to bank accounts and use of transactions in banking sphere, especially in part of payment cards; 3) methods of committing criminal offences related to the use of other means of access to bank accounts.

These include, for example, inputting false information into the banking institution's automated system; placing a bogus message on an electronic bulletin board or online auction; unauthorized interference with the on-board computer of the vehicle in order to mislead the performance. Varieties of fraud have the following features: sending an unauthorized by the legal cardholder request to make a payment and using the existing payment system and established rules for automated processing of requests of legal cardholders, the attacker spoofs the banking institution (issuing bank) about the need to fulfill the obligations under the agreement concluded between the bank and the authorised cardholder; as a result of such misleading, the issuing bank unreasonably debits non-cash funds from the account of the authorised cardholder, which leads to causing the latter losses in the form of reducing the amount of non-cash funds on the card account; the actions of the perpetrator in initiating the transfer of non-cash funds and the following socially dangerous consequences are causally related. Misleading is the defining circumstance that distinguishes fraud from other mercenary crimes against property.

Socially dangerous encroachments on property, which are committed with the use of payment cards or their details and which, in the end, lead to unauthorized transfer of funds from accounts, are grounds for classifying them not as theft (Criminal Code of Ukraine, 2001; Article 185), but as fraud (according to Article 190 of the Criminal Code). For example, a bank employee, when processing documents for issuing consumer loans to purchase goods, having access to an automated banking system, used their data and opened current accounts in the name of her customers with set credit limits. She activated instant credit cards on open accounts, with the help of which she withdrew cash through self-service ATMs. However, we

believe that all other types of such encroachments (using an ATM, payment terminal, Internet) should not be considered as a crime against property of only one kind - fraud. Thus, illegal operations with use of electronic computer equipment should be distinguished from cases of use of such equipment as a tool of commission of usual (unskilled) fraud.

For example, the use in fraud of a counterfeit document, made with the help of specialized software, should not be considered as fraud committed through an illegal transaction using electronic computing equipment. In other words, if certain technique makes possible operations that can be performed with the help of another technique (typing, document issuing, etc.), then the qualifying feature of fraud is absent. This type of fraud may require additional qualifications under Articles 361-363[1] of the Criminal Code of Ukraine. In particular, additional qualification under Article 361 of the Criminal Code of Ukraine is required for fraud committed by initiating an unauthorized transaction in the payment system on behalf of the victim, in cases where the details necessary for the transaction were obtained through unauthorized interference with the computer network (for example, "Hacking" of the email box). However, there are no signs of criminal offence under Articles 361-363[1] of the Criminal Code of Ukraine, if the perpetrator acts without illegal distorting or suppressing computer data, without causing other damage to the operation of computer facilities, uses them on a regular basis. Examples of such acts are fraud committed using the information system of an online auction or electronic bulletin board, withdrawal of cash from an ATM using a stolen payment card, and so on.

Procuring of another person's property by deception in the form of: registration on the website of the online auction providing it with inaccurate information about oneself and further placement of advertisements about selling goods or providing services that actually will not be delivered or provided for to the buyer; offers to sell non-existent goods or services using a page created on a social network; organization and maintenance of own online store, which spreads inaccurate information, etc.

In countries such as the United States, the United Kingdom, France, and Germany, the legislator considers computer crimes to be actions in which the computer is the object or instrument of encroachment (theft of computers or their components). In other countries the Netherlands, the Republic of Belarus, computer crimes comprise a separate group of crimes - illegal actions in the field of automated information processing with the main classifying features: common methods, tools, objects of encroachment; the subject of encroachment is information processed in computer system, and the computer serves only as an instrument of encroachment. The national legislation of Ukraine does not yet define the concepts of "computer crime", "computer fraud", "cybercrime", "cyber fraud'. In Articles 163 and 190 of

the Criminal Code of Ukraine (Azarov, *et al.,* 2018), as well as in Section XVI of the Criminal Code of Ukraine the terms "computer", "electronic computing equipment", "electronic computer" is defined as one and the same object of encroachment or instrument of committing a criminal offence using the Internet and computer and telecommunication devices, systems, or networks.

Thus, Article 163 of the Criminal Code of Ukraine criminalizes "violation of privacy of correspondence, telephone conversations, telegraph or other correspondence transmitted by means of communication or computer", i.e. the term "computer" is used without providing a meaningful definition. At the same time, part 3 of Article 190 of the Criminal Code of Ukraine which defines fraud as the one committed through illegal transactions using electronic computers, does not provide a definition of this term either. It should be noted that a cyber-system can be considered identical to a computer system, the definition of which is given in the Convention on Cybercrime (2001): "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

Completely new opportunities based on the characteristics of email, newsgroups and services provided by the World Wide Web are opening up to fraudsters in the area of creating "financial pyramids", sham marriage offices, employment offices, alleged service companies. In all these cases, the new tools provide with a huge speed of interaction with potential victims and anonymity of the scammer. Another type of fraud consists of modifying the algorithms that determine the functioning of the system for processing information about non-cash bank payments.

4.2 Electronic fraud with exchange rates

There are reported cases when the conversion rate has been changed. While the currency is transferred to the bank's clients at an undervalued exchange rate, the difference is transferred to accounts controlled by criminals. There is also a method based on rounding out the interest charged on a deposit of the bank's client when it is paid out, and the difference between the due and accrued (rounded) interest is transferred to the account of the offender. Such transactions, due to small amounts that are being stolen, at first may not be even detected by both clients and the bank's management. There emerged a new means of payment, the so-called electronic cash, which accompanies new types of fraud, first of all electronic cash in the form of credit cards, which are used both to get traditional paper money and to purchase goods and pay off for services with the aid of special equipment. Virtual stores are actively using a kind of e-cash in the form of electronic coins (cibercash) (Jakobsson *et al.,*2005).

4.3 The cyber fraud in social networks

Nowadays more and more types of fraud aimed at misappropriating another person's property are being invented, while information is the key to gaining access to money, because people pay online much more often than before, so more and more information about us enters the network. Social networks like Facebook, Vkontakte, LinkedIn, Instagram, Swarm, as well as programs for online communication like Skype, Viber, WhatsApp have become extremely popular. On social networks, people provide information about their place of work, date of birthday, contacts, post their photos, and start making friends. For fraudsters, intelligence services and law enforcement agencies, such information is really worthy. For example, there has recently come into being a type of fraud in which attackers copy all the information from a page on a social network, then launch subsequent web page with the same name and photos and send messages to friends of the person asking to borrow or transfer a certain amount of money.

Therefore, first of all, it is necessary to post the information within acceptable limits so that outsiders cannot find out too much (for example, phone number or postal address), or restrict access to sensitive user's information referring to the appropriate options in the settings. One should know personally all "friends" in social networks, although the marketing reality makes changes in the private character of our pages. Secondly, if you receive a friend's message the content of which seems to be strange, ask him/her something that only your friend may know, so his/her answer can make it clear that you are talking to a friend or a stranger. Fraudsters often send messages through social networks and e-mail, the content of which may look strange.

For example, it can be a message about winning of your e-mail in the lottery. Then the scammers try to obtain your personal information referring to the lottery conditions. Fraudsters can both invent non-existent lottery companies and redirect you to legitimate ones. There is always something strange about such messages, for instance, poor spelling, grammar or stylistic errors, or mistakes in an email address that does not contain any information about the sender of the message. If you do not voluntarily provide information about yourself in an e-mail, fraudsters can obtain such information by offering you to download certain programs or clicking on links. In this case you should keep in mind your own informational security and not respond to such offers/provocations.

The most popular methods facilitating fraud are computer viruses (malware), deception of the user with the intent to fraudulently acquire sensitive information from victim (for example, bank card details, etc.), offers of high-paid work at home from unauthorized employers. As well as online begging – the ads from charities, shelters, and parents asking for financial aid for the treatment of their sick children may appear online.

Scammers can make up stories about illnesses by illustrating them with photos of other people's children, or create duplicate ads for real charities, which are exact copies of the real ones, but with the bogus account details for transferring money.

4.4 The fraud to using plastic cards

Despite the various methods of protection used during the issuing and using plastic cards, there are numerous methods of fraud with them. In this case, the role of fraudsters can be 'played' both by service personnel involved in the processing of relevant financial transactions, as well as by outsiders at various stages of card usage. For example, abusing the trust of people the scammer persuaded them to "profitably" invest in e-commerce and gullible citizens transferred money from their e-wallets or through payment terminals "Web Money" to the fraudster's credit cards. (They were promised quick earnings with a solid interest after financial transactions in a virtual enterprise, but in fact people transferred money to the accounts of one of the book-maker's offices).

Also, one more type of fraud with counterfeit credit cards is based on the interception of information in the form of a pair of numbers - the credit card number and its PIN-code.

This may happen either at the stage of sending out the cards to the consumers, or at the moment of entering the PIN code in the trading terminal or ATM, or at the moment of transmission of similar information from the communication channels by the electronic terminal. Besides, the credit card number and PIN may be stolen from the bank or service organization. After the "stealing" of a credit card's identification pair, as a rule, a counterfeit plastic copy of the credit card is made and with its help a "mysterious withdrawal from the account" is made. Another possibility of "mysterious withdrawal from the account" is based on fraud of the unscrupulous personnel performing financial transactions of the client and consists in adding to them non-existent expenditures.

The second group of plastic card fraud involves the use of a phantom card. These frauds are based on the use of the uncovered algorithm to obtain the PIN code from the credit card, the issuing of a non-existent plastic card, followed by financial transactions with it.

The third group consists of fraud with real credit cards. It comprises fraud with stolen or lost credit cards, as well as various fraud committed using special techniques. (Scammers open many bank accounts with debit credit cards depositing a small amount of money on one of these credit cards. Most banks allow overdraft on debit cards to attract customers, so if the account is not closed in the bank, the money from the first card is

withdrawn entirely with overspending and transferred to the second card, from which in its turn it is withdrawn and transferred to the third one, and so on and so on. As a result of these operations a significant amount of money is accumulated).

The fourth group includes methods based on the use of bogus ATMs and trading terminals (Scammers installed a bogus ATM, accepting actual credit cards and intercepted PIN codes entered by credit cards holders. Also, they stole cash that clients tried to deposit via this ATM to their bank accounts. If people tried to get cash from this bogus ATM there appeared a message that the ATM is not loaded with bills of the required value while the neighboring ATMs were out of order) (Lysoded, 1999).

4.5 Problems to legal qualification of offenses committed using a latest technologies

Fraud, which is committed using the latest technologies, is characterized by a variety of forms and methods. However, part 3 of Article 190 of the Criminal Code of Ukraine does not reflect all possible ways of committing fraud with the use of computer equipment, the Internet, mobile communication, etc. In this respect it could be mentioned that telephone fraud is not criminalized either, i.e. when a criminal uses a telephone connection and a tool of gaining access to such connection with the intent of committing fraud: unauthorized debiting of funds from the account of a subscriber; illegal request to call on a certain phone number without warning about debiting of money during such a call; illegal transactions with topping up of mobile telephony subscribers' accounts. SMS-phishing, also known as SMiShing (from "SMS" and "phishing"), is becoming more common. Scammers send messages that contain a link to a phishing site.

Entering it and entering his/her personal data, the victim in fact transmits it to attackers. The message may also ask to call back to fraudsters on a certain number to solve "problems that have arisen." Phishing is a form of Internet fraud that allows to fraudulently obtain valuable information by spoofing communications as if they came from a reliable source, and then the information can be used to gain access to devices or networks. Targeted phishing is a targeted phishing attack based on the victim's personal information to make the attack more successful. In general, there are many types of "phishing": Creating fake web links. International Domain Names (IDNs) can be used to create confusingly similar domain names, allowing to use non-ASCII symbols. Visual similarities between symbols in different scenarios, called homoglyphs, are used to create domain names that can't be visually differentiated, and this misleads users to take one domain for another. Voice and text phishing.

To obtain account information, attackers use phone calls and text messages. At first they send messages to bank clients claiming that their accounts have been blocked. Substitution of websites, forgery, and redirection of messages (websites are vulnerable to cross-site scripting XSS) are used by attackers to post their own content on another website. An XSS attack can be used to intercept data entered on a compromised site (including user's name and password) that attackers will use later (Abroskiv, 2019). Researchers distinguish other types of "phishing", such as keyloggers and screenloggers. Letters allegedly sent from the bank may notify users of the need to call a certain number to resolve problems with their bank accounts. This technique is called vishing (voice phishing). After calling the indicated number, the user hears the instructions of the answering machine, which suggests entering account number and PINNING code. In addition, the Vishenries may call the victims using fake numbers and impersonating the representatives of official bodies (Sabadash, 2011).

There are also technically sophisticated methods based on connection to communication channels, interception of keys that provide cryptographic protection of information, and imitating the work of either an ATM (through transferring the stolen money on the fraudster's accounts), or a bank (through confirming the correctness of cash payments from non-existent accounts).

The use of credit cards on the Internet also provides wide opportunities for fraud. The exchange of plaintext on the Internet (like ordering by telephone), when all the information necessary for a purchase by credit card (card number, name and address of the cardholder, card expiration date) is transmitted openly, can be intercepted by special filters.

When exchanging encrypted messages, the sensitive information cannot be intercepted during the transmission process, but it can, however, be obtained from the seller's or buyer's server. Using clearing payment systems, when making a purchase, the customer does not provide his details to the seller, but instead provides his virtual name and credit card number, and the store authorizes the credit card not in the bank but in the clearing house. In fact, the system guarantees payment to the store, and the client provides his data to the clearing house in any reliable way, for example by mail.

The client's money from the bank is deposited in the clearing house in one of the acceptable ways (based on the client's credit card details, a transfer, or a check, etc.). While committing this type of fraud the scammer may use software that allows the perpetrator (by finding random numbers, passwords, random coincidence/selection) to obtain unauthorized access to the information stored or processed in automated systems with the purpose of misleading the automated system and impersonating oneself an authorized person to perform legitimate operations.

4.6 Means and object of electronic fraud

Thus, there are the following ways used by scammers to seize the funds of authorized payment cardholders: technical devices that are installed on the ATMs in order to seize the payment card or money; electronic devices that allow to obtain the necessary information from the payment card or from the ATM keyboard; infecting computers with viruses in order to obtain information about payment cards (by forging or hacking sites, using botnets and sending malicious spam); forgery of payment cards using stolen information; telephone fraud (when criminals act on behalf of bank employees and try to obtain the necessary information).

There are many types of fraud with payment cards and ATMs (phishing, farming, tracing, skimming, trapping, phantom, shutter, shimming, etc.), but all of them are aimed at stealing money, payment card or its details, such as: card number; date of issue/expiration of the card; CVV2 code (three-digit number on the back of the payment card, serves as a confirmation code for transactions performed on the Internet or by phone); the client's first and last name in Latin; PIN code. Besides, stolen information can be used by criminals not only to forge a payment card or debiting money, but also put up for sale on specialized sites or forums. In this case, the perpetrator may influence the processing of information, distort its content, or destroy, set the necessary command to seize property or the right to it, adjust the system so that it operates in a way that would ensure the perpetrator or his accomplice procuring, without right, someone else's property or right to it. In this case, the essence of fraudulent deception remains unchanged.

The decisive role in defining fraudulent actions belongs to the means through which it is committed - electronic computers. Thus, means of electronic communication (computer technique) includes hardware and software. Hardware includes: 1) computer (including server, personal computer); 2) peripheral; 3) digital media which includes software (system, application software, programming tool) and digital data. Software can be considered both as part of a computer system and as a separate one, for which a computer is an environment. As for the subject of ownership, which consists of property or the right to it, after the fraud has been committed, the fraudster becomes the owner of this property, or the fraudster gets the right of ownership for the subject of property right. The subject of fraud is identified with the subject of property relations, because the social connection, the normal procedure for exercising property rights is violated. Namely, the social connection in this relationship consists in the normal functioning of computers, systems and computer and telecommunication networks.

The subjects of this relationship are persons who use computers, computer systems and computer and telecommunication networks in their own interests, as well as persons who provide relevant services in this

sphere. The objects of this relationship are computers, computer systems and computer and telecommunication networks. Thus, when committing a computer-related fraud, the encroachment is made not on the normal functioning of electronic computers, computer systems and computer and telecommunication networks, but on public property relations, money and other valuables which are the purpose of misappropriation. The object of the fraud in question may not be computers, computer systems and computer networks and telecommunication networks.

4.7 Subject of electronic fraud

As for the subjects of these relations, such fraud can be committed by any persons using computers, computer systems and computer and telecommunication networks in their own interests, as well as by persons who provide relevant services in this sphere. At the same time, while committing such fraud, these persons perform legal operations using electronic computers, without disrupting the normal functioning of electronic computers. Thus, the use of electronic computers with the purpose of misappropriation of someone's property is criminalised under Article 190 of the Criminal Code of Ukraine.

4.8 Remote banking services

Remote Banking Services (RB) is a general term for technologies providing banking services on the basis of orders transmitted by the client remotely (most often without his direct visit to bank). The RB system is a multi-functional software and hardware complex that allows the bank's clients to prepare and send payment orders and other documents to the bank for performing, to view account balances, as well as to receive a wide range of relevant financial information without contacting the bank. Interference with the operation of RB systems occurs by infecting the computer with malware via malicious spam, visiting infected sites or using infected magnetic based memory. The main task of the virus at the initial stage is to monitor and collect information and transmit it to the computer of fraudsters.

The virus can obtain access to passwords to RB systems, electronic 16 digital signature keys, read payment details. There may also be programs that track connection window to RB with the intent of further interception of the secret information which is entered in this window, or copy content of the clipboard at the moment of connecting to systems of electronic payments. The purpose of fraudulent actions is to distort information, generate (with the help of RB) and make a payment that will look like an ordinary payment of the victim, while scammers will transfer money to

the accounts of a fictitious person or fictitious firm, trying to feature the usual payments for usual purchases of the client. Later on, most often the money stolen from the victim's account is transferred into cash, and cash withdrawals are carried out mainly through ATMs in order to avoid communication with bank employees (Kornienko and Strelyany, 2015).

4.9. Cyber fraud can be divided into the following categories:

cyber fraud with the intent of misappropriation of funds.

cyber fraud with the intent of obtaining information (for personal use or for resale);

in the banking system:

1) *ATM fraud:* skimming - making, selling, and installing on ATMs devices for reading/copying information from the magnetic strip of a payment card and obtaining a PIN code to it (illegal copying of the contents of magnetic strip tracks (chips) of bank cards); use of "white plastic" for "cloning" (counterfeiting) of a payment card and cash withdrawal at ATMs; cash trapping - theft of cash from an ATM by installing a special restraining pad Transaction Reversal.

Fraud on the ATM tent - interference in the work of the ATM during cash withdrawal operations, which preserves the balance of the card account unchanged while in fact the attacker has already received cash; Cash Trapping - sealing the dispenser for misappropriation by the attacker of cash that was debited from the card account of the authorized cardholder; - carding - illegal financial transactions using a payment card or its details, which are not initiated or confirmed by its holder; - unauthorized debiting of funds from bank accounts using Remote Banking Systems.

2) *fraud in marketing and service networks*: concluding fictitious trade acquiring agreements for servicing counterfeit payment cards; obtaining payment card details, including the use of technical means for their "cloning"; online fraud – misappropriation of citizens' money through online auctions, online stores, websites and telecommunication means; transactions with the amounts of money below the established limit without authorization; use of lost/stolen/ counterfeit payment cards.

3) *fraud on the Internet*: obtaining, without right, of payment card details; phishing - luring of Internet users' logins and passwords to e-wallets, online auction services, currency transfer or exchange, etc.; performing operations with the use of stolen payment card details; creating malware with the intent of obtaining, without right, payment card details (via bogus WEB-sites, dissemination

of computer viruses and Trojan programs, interception of traffic); malware - the creation and dissemination of viruses and malware; re-filing - illegal substitution of telephone traffic.

4) *fraud in remote banking systems (RB):* creation of computer viruses and Trojan programs for covert interception of the client's computer control with the installed RB software; opening accounts, performing unauthorized transactions and receiving cash as a result of unauthorized transactions in RB systems; receiving payments from foreign senders via the international SWIFT system as a result of interference in the work of computers and RB systems of clients of foreign banking institutions (Order, 2013).

According to Part 1 of Article 190 of the Criminal Code of Ukraine, fraud is misappropriating of someone else's property or taking possession of the right to property by deception or abuse of trust. From the point of view of juridical psychology, fraud means manipulating a person's behavior to obtain a quick and maximum profit from him, and from the point of view of jurisprudence, fraud is the misappropriation of individual property or taking possession of property rights by deception or abuse of trust (Azarov, *et al.*, 2018). In criminal law the deception is understood as the informational and intellectual influence of one person on the consciousness and will of another, which is always aimed at certain behavior, i.e. to induce the victim to a certain behavior. Deception is a way of influencing the human mind, which is deliberately luring another person or maintaining delusion through misinforming or non-informing about various facts, things, phenomena, actions and others in order to induce certain behavior. Deception in fraud can consist in the use of software that allows the perpetrator to gain unauthorized access to information stored or processed in automated systems, with the intent of impersonating an authorized person. Having penetrated in this way into the relevant electronic system, the perpetrator performs certain operations, as it would do the authorized person.

Herein, he may hinder, without right, the processing of information, distort its content, delete or destroy or set the necessary command to defraud property or the right to it, set up the system so that it operates in a way that would ensure the culprit or another person illegal misappropriation and loss of property or right to it. The essence of fraudulent deception remains invariant, the only thing is the fraud is committed using electronic computers and technologies, which require more elaborate and innovative techniques, training, skills.

Another type of fraud according to Article 190 of the Criminal Code of Ukraine is *abuse of trust*, i.e. intentional actions of the offender aimed at luring the victim using existing or new personal or other trusting relationship with the intent of defrauding and procuring an economic benefit for oneself or for another person from victim's property or property rights. Abuse

of trust as a method of fraud with the use of electronic computers occurs when the guilty person makes use of trusting relationship (official relations, friendly relations, etc.) and has free access to the relevant operations and abuses these relations with the intent of misappropriation of property or the right to it. If the perpetrator enters the secure electronic system, for example, by blocking or destroying security codes, and performs illegal transactions to misappropriate someone's property or property rights, his actions do not constitute fraud because there is no deception or abuse of trust. They should be prosecuted as theft of someone's property and criminalized under the relevant part of Article 185 of the Criminal Code of Ukraine.

4.10 Proposals of legal regulation and countering cyber fraud

It should be noted that the term 'fraud' is inappropriate to use in legal definition of socially dangerous actions the essence of which is in entering, altering, disrupting, destroying or suppressing computer data in the computer, automated system, computer network or telecommunication network, or is characterized by any other influence on the processing computer data that has changed the result of this processing, with the intent of misappropriating someone's property, because the fraud always encroaches the ownership and is followed by the voluntary transfer of property while the influence on computer information is coercive and doesn't involve the influence on the victim's conciseness.

First, a computer network (including the Internet) is by definition a set of geographically dispersed data processing systems, facilities and (or) communication and data transmission systems that provide users with remote access to and sharing of its resources (UN, 2010). Accordingly, the posting of the message on a specialized website means the use of information resource via remote access to it, which is provided with means of electronic computing, i.e. is an operation using an electronic computer.

Secondly, under Article 19 of the Law of Ukraine "On Consumer Protection" (1991): posting a knowingly false information about the sale of goods or provision of certain services is a dishonest business practice and is prohibited, and criminal law characteristic of fraud committed by posting such information on relevant Internet resources, is criminalised under Part 3 of Article 190 of the Criminal Code of Ukraine "Fraud committed through illegal transactions using electronic computers", so it is necessary to establish in the Criminal Code of Ukraine the following rule:

"Theft of property through the use of electronic computers." Criminals mostly use special malicious programs or technical means (in particular, the Code of Laws of the United States, the Dutch Criminal Code of the Netherland, the Criminal Code of Denmark or the Criminal Code of FRG

refer to it) and the introduction to part 3 of Article 190 of the Criminal Code of Ukraine amendment "by means of malware or malicious hardware "shall become an additional instrument for combating" cybercrime" (Shulyak, 2011).

Punishment for fraud shall be economic, monetary and the main sanction for such crimes should be a fine, and as an alternative (in cases where the perpetrator does not want to pay the fine, does not have money to pay it or has no property by which to pay a fine) - correction works or deprivation of the right to hold certain positions or engage in certain activities for up to three years - for officials; confiscation of relevant malicious software or hardware that are in property of the perpetrator, if they were used during the commission of fraud.

Now, it can be stated that the current rule (Criminal Code of Ukraine, 2001: part 3 of Article 190) can work effectively if it is correctly interpreted and applied, as fraud in this case implies entering into computer, automated system, computer network or telecommunication network of false information, because, firstly, the computer does not store money or property, but only information about this property or transactions with this property; secondly, if the perpetrator even secretly enters a computer system with the intent to obtain, without right, money or property, it is done through the manipulation with programs, data or hardware, which is typical for deception, which is specific to computer fraud (for example, a person, having access to the automated system of a banking institution, inputs or alters computer information, as a result of which, the money is transferred from the victim's account to perpetrator's one), while the relevant protective (security) systems or computer programs interpret this false information as if it were at the victim's own request or on his personal behalf).

It should be noted that from 1 August, 2016, the Visa payment system introduced in Ukraine the principle of zero customer liability for fraudulent actions (banks will return money stolen by fraudsters to Visa cardholders). Measures taken by Ukrainian banks to prevent fraud include monitoring, SMS-informing, banning Internet payments without a phone call to the bank, setting limits on cash withdrawals and payments (in particular, on the Internet). A bank card with a computer chip is the most secure, as it is much more innovative than magnetic strip cards, as they cannot be counterfeited, and the data of such card cannot be copied by fraudsters. Banks monitor the security of ATMs for fraudulent installation of additional reading devices, equip ATMs with anti-skimming pads on the card acceptor, video surveillance, etc. General rules and recommendations for users are: mandatory connecting to 3D Secure service, SMS - and mobile banking; storing of cards and passwords separately; avoiding of payments on the Internet by the card on which the basic funds are accumulated;

non-disclosing of card details to the third persons, periodic (once a month) password changing; setting payment limits in the retail network and the Internet; complete blocking of card payments on the Internet; non-disclosing security codes CVV2/CVC2; receiving a card with a chip (Makarova, 2016).

In order to take into account certain provisions concerning illegal transactions with means of payment, such as bank payment cards, it is appropriate to focus on the Council of Europe Framework Decision "On Combating Fraud and Counterfeiting Non-cash Means of Payment" (CF, 2001). In accordance with the provisions of this document, the following crimes related to means of payment are distinguished: 1) theft or other illegal misappropriation of a means of payment; 2) forgery or falsification of a means of payment with the intent of using it in fraud; 3) acceptance, receipt, transfer, sale or transfer to any person or possession of a stolen, or otherwise misappropriated, or counterfeit or falsified means of payment with the purpose of its use in fraud; 4) fraudulent use of a stolen, or otherwise misappropriated, or counterfeit or falsified means of payment. The implementation of the provisions of the EU Directive 2007/64 (EP, 2007) has significantly influenced the regulation of activities to prevent criminal encroachments committed with the use of bank payment cards.

However, one of the reasons for the high latency of cyber-fraud is 'the absence of state borders' if this criminal offense is committed via the Internet, imperfect legislation and, consequently, the inability to cooperate with other countries in investigating such criminal offenses because of significant differences in legislation of different countries regarding this type of criminal offence.

Also, we suggest the main ways for combating fraud on the Internet committed using electronic computers: development of new software and constant renewal of antivirus programs; creation of the system of authentication of Internet addresses for checking the conformity of the address entered by the user to the real server; greater spreading of information about known methods of Internet fraud to Internet users. In order to prevent payment card fraud, the National Bank of Ukraine shall improve and spread, on permanent basis, recommendations for payment card holders on their use.

Conclusions

Summing up, it can be noted that our survey based on questionnaire of law enforcement officers, analysis of law enforcement practice, existing scientific publications, and legal regulations, helped specify the most common in Ukraine methods of computer-related fraud, provided them with criminal law characteristics and suggested measures for counteracting these criminal offences.

We provided reasons for clarifying the features of computer-related fraud. Illegal transactions using electronic computers should impose as those aimed at misappropriating someone's property or property rights, which are based on deception or abuse of trust, i.e. fraud using computer networks, despite evolutionary processes, remains a crime against property committed through deception or abuse of trust. And deception occurs not during direct physical verbal or non-verbal contact with the victim, but remotely, i.e. using the capacity of computer and telecommunication devices, systems or networks.

The danger of such fraud is that computer techniques greatly facilitate fraud, allows someone to misappropriate significant funds, causing irreparable damage to owners. Public relations of any form of ownership are the direct object of fraud committed through illegal transactions using electronic computers. Public relations in the field of the use of electronic computers, telecommunication networks can be neither generic nor direct object of such fraud. It should be noted that operations with electronic computers during the commission of fraud in most cases are quite legal and legitimate, for example, the use of the Internet, telecommunication network. Based on the above, it can be concluded that the object of fraud committed via illegal transactions using electronic computers is property relations and committing of such fraud is carried out by a person who is not the owner. As for the subject of property relations, which is property itself or the right to it, after the fraud has been committed, it becomes the property of the fraudster, or the fraudster obtains the right of ownership for the subject of property relations. Fraud is an intentional criminal offence, and the perpetrator wants the result – procuring, without right, certain property for his benefit. As for the lost profit, the guilty person, as a rule, has no direct intent, and this excludes the possibility of recognizing this consequence as an element of any form of theft.

Acknowledgment

Authors thank the Department of Cyber police of the National Police of Ukraine for participating in the sociological research.

Bibliographic References

ABROSKIV, V. 2019. Cyber security in Ukraine: Legal and Organizational Issues. ODUVS. Odessa, Ukraine. Available online. In: http://eportfolio.kubg.edu.ua/data/conference/5087/document.pdf. Consultation date: 11/03/2020.

AZAROV, D. 2007. Crimes in the Field of Computer Information (criminal law research). Atika. Kyiv, Ukraine.

AZAROV, D.; GRISHCHUK, V.; SAVCHENKO, A. 2018. Scientific and Practical Commentary on the Criminal Code of Ukraine. Ed. by O. Dzhuzha, A. Savchenko and V. Cherney, Yurinkom Inter. Kyiv, Ukraine.

COUNCIL FRAMEWORK EU. 2001. "Combating fraud and counterfeiting of non-cash means of payment", Decision No. 2001/413/JHA. Available online. In: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001F0413. Consultation date: 11/03/2020.

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME. 2001. Ratified with reservations and statements by the Law of Ukraine "On Ratification of the Convention on Cybercrime" No. 2824-IV. Available online. In: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_575. Consultation date: 11/03/2020.

DUDOROV, O. 2014. "Problems of Qualification of Fraud". Available online. In: http://law-dep.pu.if.ua/conference2014/articles/dudorov.pdf. Consultation date: 15/03/2020.

EUROPEAN PARLIAMENT AND OF THE COUNCIL. 2007. "On payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC", Directive 2007/64/EC. Available online. In: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0064. Consultation date: 11/03/2020.

FINAGEEV, V. 2016. "Ways of Committing Crimes Related to the Use of Means of Access to Bank Accounts" In: Scientific Bulletin of the National Academy of Internal Affairs. No. 1, pp. 63–82.

JAKOBSSON, Markus; JAGATIC, Tom; STAMM, Sid. 2005. "Phishing for clues: Inferring context using cascading style sheets and browser history". Available online. In: http://www.browser-recon.info. Consultation date: 11/03/2020.

KARCHEVSKY, M. 2012. "Peculiarities of the Qualification of Crimes Against Property Committed with the Use of Computer Equipment" In: Business, Economy and Law. No. 1, pp. 139–142.

KORNIENKO, V.; STRELYANY, V. 2015.Investigation Procedures of Facts of Unauthorized Transfer of Money from Bank Clients' Accounts, who are Served by Remote Service Systems. Kharkiv, Ukraine.

LAW OF UKRAINE. 2001. Criminal Code Of Ukraine: No. 2341-III. Available online. In: http://zakon.rada.gov.ua/laws/show/2341-14. Consultation date: 10/03/2020.

LYSODED, O. 1999. "Criminological Problems of Fraud" Thesis abstract for PhD in law. Yaroslav the Wise National Juridical Academy of Ukraine. Kharkiv, Ukraine.

MAKAROVA, L. 2016. "Visa Introduces the Principle of Zero Customer Liability for the Actions of Fraudsters". In: Debet-Credit. Available online. In: https://news.dtkt.ua/finance/banks/39582. Consultation date: 11/03/2020.

MUZYKA, A.; AZAROV, D. 2005. Legislation of Ukraine on Criminal Liability for "Computer" Crimes. In: Scientific and Practical Commentary and Ways to Improving. Publishing House PALYVODA A.V. Kyiv, Ukraine.

ON CONSUMER PROTECTION. 1991. Law of Ukraine No. 1023-XII. Available online. In: https://zakon.rada.gov.ua/laws/show/1023-12#Text. Consultation date: 11/03/2020.

ORDER. 2013. "About the statement of Typologies of legalization (laundering) of the incomes received by a criminal way, in 2013" No. 157, [Appendix "Cybercrime and money laundering"]. State Financial Monitoring Service of Ukraine. Available online. In: https://zakon.rada.gov.ua/rada/show/v0157827-13#Text. Consultation date: 11/03/2020.

SABADASH, V. 2011. "Fraud in electronic commerce: today's reality" In: Bulletin of Zaporizhia National University. No. 1, pp.216-220.

SHAPOCHKA, S. 2015. "On the Concept of Fraud Committed Using Computer Networks (Cyber fraud)" In: Bulletin of the Association of Criminal Law of Ukraine. Vol. 4, No. 1, pp. 221-232.

SHEVCHENKO, V.; SHULYAK, Yu. 2018. "Theoretical and Legal Features of Illegal Criminal Transactions with the Use of Computer Technologies" In: International Journal of Innovative Technologies in Social Science. Vol.3, No. 4(8), pp. 80-83.

SHULYAK, Yu. 2011. Criminal Liability for Fraud: a Comparative Legal Study. Thesis abstract for PhD in law. National Academy of Internal Affairs. Kyiv, Ukraine.

UNITED NATIONS. 2010. On Crime Prevention and Criminal Justice, Twelfth United Nations Congress, 2010, Salvador, Brazil. Available online. In: http://www.unodc.org/documents/crime-congress/12thCrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf. Consultation date: 11/03/2020.

VASYLIEV, A.; PASHNEV, D. 2013. "Peculiarities of the Qualification of Crimes in Computerised Environment, Computer Systems and Computer Networks and Telecommunication Networks" In: Bulletin of the Criminological Association of Ukraine. No. 5, pp. 34-42.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.39 Nº 68

Esta revista fue editada en formato digital y publicada en enero de 2021, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org