Internet fraud and transnational organized crime

Assistant professor **Nadiia SHULZHENKO**[1]
PhD. student **Snizhana ROMASHKIN**[2]

Abstract

The present research paper describes the most traditional ways of today's mass-marketing financial crimes such as fraud. Digital banking is now used daily for checking account data, making purchases, paying the bills, transfer money, print statements, etc. Online fraud is a crime committed with on-line software to unlawfully allocate money from both bank' and payment systems' account and/or transfer money to another bank account. Banks are not so much targeted in today's world, there's a lot of money in cyberspace, in modern digital systems and data networks. The main task of this article is to determine the most common forms of online financial crimes, such as "Hacking" or electronic transmission unintended for the interceptor, such as passwords, credit card information, or other types of identity theft. The article discusses the features of legal regulation and the activities of the Ukraine to protect citizens form Internet frauds and to avoid Internet scams, phishing and other cybercrimes in Internet. In this article, we review some principles of qualitative data collection, analysis, and strategic planning to help scientists, lawyers, and law students interested in conducting research in their practice to continue their learning in this area.

Keywords: *internet frauds, banking frauds, transnational crimes, cybercrimes, phishing.*

JEL Classification: K14, K24

1. Introduction

The banking system, which operates to ensure price-policy stability, support for national currency, organization and operation of the international payment system, is given a special place in the international economy.

One of the important tasks is to protect bank clients and most people with the use of internet banking systems and credit cards from crimes committed in banking areas.

This can become a more challenging organized crime issue, as the Internet continues to be a critical part of our world. And despite widespread awareness of security problems, offenders can still find more victims and find solutions to Internet fraud by using online services as well as network-access software applications.

[1] Nadiia Shulzhenko - Department of Criminal Law № 1, Yaroslav Mudryi National Law University; senior research officer of Academician V.V. Stashis Scientific Research Institute for the Study of Crime Problems, National Ukrainian Academy of Law Sciences, Ukraine, nevidoma_n@ukr.net.

[2] Snizhana Romashkin - PhD student of Academician Stashis Scientific Research Institute for the Study of Crime Problems, National Academy of Law Sciences of Ukraine, Ukraine, snizhana.romashkin@gmail.com.

The extent to which criminals are exploiting digital technology to commit offences has accelerated. The term cybercrime refers to any type of criminal activity conducted through, or using, an Information and Communications Technology (ICT) device. Cybercrime can take place in conjunction with a variety of related criminal activity, and cyber techniques have proliferated to the more traditional criminal community, for example, urban gang members buying compromised data online.

Law enforcement institutions is continuing to develop legislation that victims can use to protect their rights. These laws were enacted to effectively highlight cybercriminals actions and create a sustainable digital world protected from fraud.

The present paper analyzes major fraud methods of activities committed with using bank payment cards. General fraud consists of fraud in general (article 190 of the Criminal Code of Ukraine), fraud with financial resources (article 222 of the Criminal Code of Ukraine) and others, defined in the Criminal Code of Ukraine. Special methods of fraud committed using bank payment cards (computer fraud). The main types of bank payment fraud include the following: phishing, which has subspecies: mixing and whisking; carding, which has subspecies: skimming, shimming; fraud with bank cards in the Internet, which has subspecies: fraudulent activities in social networks, pharming; scamming; fraud with bank cards in service sales networks.

There are two main ways of fraud: by deception or through abuse of trust. Fraud committed with the use of bank cards can be carried out in an active form, when misinformation causes misconception about the facts of the victim, leading to the loss of the victim's property, and in a passive form, when the offender doesn't notify the facts known to him to the victim, and this also leads to the loss of the victim's property. A mandatory condition for the recognition of fraud or abuse of trust as a sign of fraud committed with the use of bank payment cards is the use of it for the occupation of property even the acquisition of the right to such property by payment card. Therefore, if a fraud is used to achieve another goal and doesn't directly lead to the transfer of property (property rights), through bank payment cards, such acts shouldn't be regarded as a fraud but as a criminal offense that encroaches on property.

2. Present banking frauds cases in internet

Online banking fraud has become more popular since banks move away from branch banking and introduce more online applications. Though electing certain kind of fraud, a criminal is not influencing in general on the qualification of his actions in terms of Criminal law, however, criminals are more inventive by engaging for illegal activities in modern technologies, which leads to victims' misunderstanding. To find out the key features of behavior it is advisable for all victims to investigate the above fraudulent practices.

Banks must respond to modern electronic developments, thus protecting

their customers and their access control against online crime. Online banking fraud can take manifestations, but usually begins with phishing to get customer account information. Account numbers, credit card information can be collected using email and telephone scams. After payment or login details are collected, money can be transferred from the customer's account.

Direct or indirect fraud are two major types of electronic fraud, that could be classified nowadays. Direct fraud contains credit/debit card fraud, misappropriation of funds of employees, money laundering and target. Indirect fraud includes phishing, pharming, hacking, virus, spam, anticipation fees, and malware. Credit card/debit card fraud and identity theft are specific types of e-fraud which are often primarily used. These forms include both identity theft and impersonation (name, social insurance number (SIN), credit card number or other identifying information) to carry out fraudulent activities. It is the unlawful use of a credit/debit card to falsely obtain money or belongings without the awareness of the credit/debit card owner. Theft of someone's identity can be done in different ways. Skimming involves stealing information from a credit card during a valid transaction in the case where the customer's credit card is hidden from sight while making the transaction. The scammer will scan the card through an electronic skim device that copies all the magnetic stripe information. To extract credit card details, criminals could use advanced methods, for instance, hacking into the databases of merchants to get credit card details.

Phishing is one of the most effective means of personal removal data from Internet users and web resources. Google employees conducted a study that examined the sales of online accounts on black market. They found out that the most common cause of personal data leakage is - it's phishing. It turned out that 15% of all users have encountered fraudsters online at least once and lost their data accounts and even payment card information[3].

And while everyone tries to protect themselves and their users from hackers, it doesn't always work out. More than 800,000 passwords have been lost people through keyloggers (software or hardware) a device that records the various actions of the user - typing on the keyboard computer, mouse movement and keystrokes, etc). Through phishing attackers stole at least 12 million accounts within 2014-2016.

The main phishing attack vector is aimed at the weakest link of any modern security system - per person. Not always a bank customer can distinguish his bank's original web address from phishing copy, for example, attackers can use and the fact that in some fonts the lowercase letter — "i" is capitalized — "L" look like equally (I = l). Such methods allow to deceive the person with the help of similar to the real link in the email, even clicking on this link (to see the real

[3] Leukfeldt, Eric, *Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization,* „Cyberpsychology, Behavior, and Social Networking", 17(8), 2014, pp. 551-555.

address) does not help[4].

There are other means in the arsenal of intruders: from the substitution of the real IP address to the fake one (in Windows, for example, for this it is enough to edit the hosts file) before the pharming is a procedure the victim's secret referral to the wrong IP address).

Not wanting to incur additional costs, the Phishers simply direct their attacks for the most popular services - auctions, payment systems, big banks - in the hope that a random spam recipient has an account there.

Thus, we are able to distinguish the following types of phishing attacks:

Classic phishing. Phishing emails sent on behalf of known people really existing companies that are virtually indistinguishable from emails that users usually receive from these companies. The only difference is to ask for a link to perform some action.

Targeted phishing attack[5]. Personalized phishing emails, aimed at a specific person. Such letters contain a name, a position of potential the victim, as well as any other personal information.

Phishing against top management. Phishing emails are aimed at getting access to the account of the head of the company, CEO, technical directors, etc. After access to such accounts, specialists from phishing can continue to be used to reach other departments, for example, to confirm fraudulent bank transfers to any financial entity to an institution of their choice.

Google and Dropbox mail phishing. A relatively new direction phishing attacks aimed at usernames and passwords to log in to the cloud data warehouses.

Phishing emails with attached files. Phishing lists from attachments containing viruses.

Farming. Hidden redirect to a fraudulent site executed by changing the DNS cache on your local computer or network equipment[6].

Now let's define the basic methods of combating phishing sites and others types of online fraud.

The first is to create a unique website design for everyone user. The essence of this method is: a customer, for example, at a bank or website at contracting selects one of the proposed images. Further at the entrance to the bank's site will be shown exactly this image. If the user he does not see or see another, he must leave the fake site and immediately inform the security service. It is alleged that the abusers were not present at the signing of the contract, will not be able to guess the correct image and to deceive the client. In practice, however, this method is not critical. Firstly, in order show the user his picture, he must first be identified, for example, by the login he entered on the first page of the bank's website. For the

---

[4] Jansen, J., & Leukfeldt, E.R., *How people help fraudsters steal their money: an analysis of 600 online banking fraud cases*, Workshop on Socio-Technical Aspects in Security and Trust, 2015, pp. 24-31.

[5] Yazdanifard, Rashad & Wan Yusoff, Wan Fadzilah & Behora, Alawa & Sade, Abu, *Electronic banking fraud; The need to enhance security and customer trust in online banking*, „International Journal in Advances in Information Sciences and Service Sciences", 3, 2011, pp. 505-509.

[6] Shannak, R., *Key Issues in E-Banking Strengths and Weaknesses: The Case of Two Jordanian Banks*, „European Scientific Research", 9, 2013, pp. 239-263.

attacker is more difficult to prepare a fake site to find out this information as well for the user himself - to emulate a communication error. Now it is enough to turn on a real server, enter the stolen login and see the correct image.

The next method is to use one-time passwords. Classic passwords are available reusable: the user enters the same password each time at undergoing authentication procedures without changing it over time. Hacked by an attacker, this password can be used repeatedly without known to the owner.

Unlike the classic one-time password, only one is used once, that is, every time a request for access is made, the user enters a new one password. Special plastic cards are used for this purpose the applied protective layer. Each time a bank customer erases the next strip and enters the required one-time password. All in a standard size card placed about 100 passwords, which is intensive use of services TV banking requires regular media replacement.

More convenient, but more expensive are special devices - One-time password generators. There are basically two types of such creation: at a time when the current one-time password is displayed on the screen periodically changes (for example, every two minutes); when new value is generated every time, a user clicks a device button.

Being more secure than classic password authentication, however, it leaves the attacker with a good chance of success. For example, authentication with the use of one-time passwords is not protected against the attack of the person in the middle.

Its essence is "wedging" into the information exchange between the user and server when the attacker "appears" to the user's server, and vice versa[7].

The server transmits all information from the user, including the information entered by the user a one-time password, but on behalf of the attacker. The server having received the correct one password allows access to private information. Without causing suspicion, the attacker may allow the user to work with, for example, their account, sending him all the information from the server and back, but when completed the user of his work session is not to break communication with the server, but to do transactions are required on behalf of the user.

To avoid wasting time waiting for a user session, an attacker can simply simulate a communication error and not allow a legal one user to work with their account. Depending on the method used, the generation of the intercepted one-time password will be valid or for short time, or only for the first session, but in any case, it gives an attacker the possibility successfully steal data or money from the user[8].

Fraudsters can present themselves to bank employees, tell stories about "system issues", the need to urgently recover all customer personal information to

[7] Chavan, J., *Internet Banking - Benefits and Challenges in an Emerging Economy*, „International Journal of Research in Business Management" (IIEBM), 1(1), 2013, pp. 19 -26.

[8] Bolton, R. & Hand, D., *Statistical fraud detection: A review*, „Statistical Science", 17(3), 2002, pp. 235-255.

save money on their account or to make sure your card has not been stolen. To do this, they will be required to provide all your personal and card details.

Or they will just be asked to read the code that will come to you via SMS and, as if, will confirm that your card and everything is fine with it. But don't read what it says. After all, at this time, it is likely that the fraudsters are trying to use the cashless card service through an ATM. And all they need is the same code they require. Once it is announced, the money will be deducted from the account[9].

Another way fraudsters steal money from a bank account is to get a duplicate of the SIM card of the cardholder's mobile number. Then your phone will be locked, and fraudsters, knowing the credit card number and having a duplicate SIM in their hands, will receive all the necessary passwords and confirmation codes for online transactions, or at an ATM.

Most often victims of this method are sellers of goods online. They place ads, so they are not surprised by calls from unfamiliar numbers. In order to get a duplicate of a phonecard, the fraudsters either force the person several times in a row to call them and do not pick up the phone, or make a call themselves and cut off the connection. Thereafter, a minimal erroneous "replenishment" may come into the account. And then the number itself is just blocked. This means that knowing the information about the last dialed numbers, the last replenishment, the fraudsters ordered and received a duplicate SIM card from the mobile operator. Such situations should alert all people.

Cyberattacks are more and more likely to affect small and medium-sized businesses since such companies mistakenly consider themselves "uninteresting" in terms of information the resources they own.

When breaks affect large organizations, the latter are usually fall under the sights of the public media. However, in reality, they are only a small percentage of the total number of attacks that occur every year. In practice, 71 percent of database breaks are small businesses.

Spear Phishing and Watering Holes are the most common types of attacks. In 91 percent of cyber-attacks, phishing is the first line of attack. While traditional phishing attacks spread across a broad network, sending out emails to hundreds or thousands of recipients targeting phishing attacks (spear phishing) target small subgroups of people like as a rule, employees of companies. A scammer who plans a targeted phishing attack can create a fake email of the employee and write to him, several legitimate employees, by requesting company information. Thinking that they communicate with a colleague, legitimate employees can provide this information. And that's where the question of setting up corporate mail comes from; it is an SPF digital signature whose value determines the servers from which it is possible to send mail from a corporate domain[10].

---

[9] Omariba, Z., Masese, N. & Wanyembi, G., *Security and Privacy of Electronic Banking*, „IJCSI International Journal of Computer Science Issues", 9(3), 2012, pp. 432 – 446.

[10] Saranya, K. & Gunasri, K., *Challenges in E-Banking*, „International Journal of scientific research and management" (IJSRM), a special issue of journal with no volume or issue number, 2013, pp 22-27.

Also, important milestone security is a check of the technical title of the letter containing the information about mailing time and mail servers. So the question of coaching arises working staff on basic information security rules. Conducting such training for working staff will not lead to great cost, however, it can be quite significant.

When using a Watering Holes attack strategy, hackers place malware in the code of the websites that are the largest the employees of the attacked company are likely to visit. If an employee goes to such a site from a company computer, the entire company network may be exposed to a virus that will collect data.

The reason why small and medium-sized businesses are exposed to cyberattacks quite simple. Large organizations tend to store important data on own servers, while small and medium-sized ones rent remote servers. Small and medium-sized businesses need to become more secure. By statistics from more than half of businesses in Ukraine do not take any preventive measures to protect themselves from cyber-attacks. In addition, 85 percent do not even plan to increase their budgets by security, despite the fact that the number of attacks is increasing. It makes small and medium-sized businesses are especially appealing to hackers who prefer easy targets[11].

Logic bombs are able to access confidential information, disable the equipment. They can cause losses of personal information, the reputation of the person, international image, confidential information. With their help you can "cause catastrophes at nuclear power plants, open dams for flooding of settlements, to disable dispatching equipment for the purpose of calling aircraft crashes".

The Vishing Attack is capable of delivering financial damages to the user, steal sensitive information organization[12].

DDoS attacks are most commonly performed for commercial benefits because it takes hundreds of thousands to organize a DDoS attack computer, and such enormous material and time costs can afford not everyone. Attackers are used to organizing DDoS attacks a special network of computers - a botnet. Kaspersky Lab regularly conducts studies that show the most DDoS attacks suffer from Internet commerce, the financial sector, and IT companies.

In our opinion, the very need to strengthen security measures to counteract it Cyber fraud, in particular, is to increase the level of ordinary people's skills Internet users and financial services, as they are emerging victims of fraud. Therefore, we need to make further recommendations for reinforcement cyber-fraud security measures and user recommendations.

---

[11] Bhasin, Madan, *An empirical study of frauds in the banks,* „European Journal of Business and Social Sciences", 4, 2015, pp. 1-12.

[12] Chakrabarty, K., *Fraud in the banking sector – causes, concerns and Cures.* The National Conference on Financial Fraud organized by ASSOCHAM, July 26, 2013, New Delhi, India, pp 1-13. The document is available online at: http://rbi.org.in/scripts/BS_Speeches View.aspx?Id=826 (consulted on 1.10.2019).

3. Practices of Google in counteracting phishing attacks

Gmail's security has been further enhanced with more care. Tracking Google sign-in through third-party applications. That's how it worked Google Docs attack - instead of cloud office suite, users were logged in a fake application that requested your Google Account login and password.

An advanced spam filtering system has also been added. In addition, the company already has a number of anti-phishing activities are machine-based fraud detection training, Safe Browsing mode, email attachment scanning and more security measures for suspicious Google sign-in.

Google also uses its own Safe Browsing API secure search, application programming interface, application interface programming, English. Application Programming Interface (API) allows applications from client-side to check that the URL is blacklisted constantly Google is being updated. Although the protocol is still experimental, most browsers do use it. The list is maintained on the client-side and periodically updated; however, if the URL is changed even slightly, then the URL is gone will be blacklisted.

Because the life of these phishing attacks is very short, there is a lot of data used to store these blacklisted and domain URLs, which will be of no use in the near future. In addition, the complexity the comparison of each user URL with blacklist data is very high.

The most common vulnerability to phishing attack methods is using URL blacklists is what information security is still faces the fact that attackers can still access the site simply changing the IP address or using bots to fake the domain[13].

New methods of counteracting cyber fraud can also be added implementing e-mail security already in place mechanisms - SPF, DKIM, DMARC and others. According to Gartner, in the Top 5 appropriate the market segment today includes the following companies: Barracuda Networks, Cisco, Mimecast, Proofpoint and The Email Laundry.

The second line of defense is usually considered access control means Internet - local or cloud. They allow you to block conversions by mail, SMS or MMS links (in the last two cases required cloud solution - perhaps on the side of a mobile carrier or a specialist information security service provider). Among the leaders in this segment you can name Bluecoat, Cisco, Websense and Zscaler[14].

4. Ukrainian practice on combating online organized crimes

According to the Law of Ukraine "On the organizational and legal bases of the fight against the organized criminality" system of state bodies which combat

---

[13] Vrincianu, M. & Popa, L., *Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests*, „Amfiteatru Economic" no. 12(28), 2010, pp. 388-403.

[14] Kovach, S. & Ruggiero, W., *Online Banking Fraud Detection Based on Local and Global Behavior*, The Fifth International Conference on Digital Society, Guadeloupe, France, 2011, pp. 166-171.

organized crime, are:

a) specially created for the fight against organized crime state bodies;

b) state authorities involved in the fight organized crime within execution other major functions assigned to them. From number of subjects of the specified activity by questions prevent online cryptocurrency fraud. The competences defined on the basis of the relevant laws can be distinguished as follows: National Bank State Tax Service of Ukraine, Security Service of Ukraine, Ministry of Internal Affairs of Ukraine[15].

Accordingly, there may be threats that are subjective in nature casual or intentional. However, self-defense is used for preventing the intentional act of the attacker. O.I. Karpenko includes following statements to self-protection: encryption, electronic watermarks, passwords, malware distribution bypassing technical protection methods. Technical protection of information involves the use now hardware, software, cryptographic and other methods and tools for exclude unauthorized users and applications from accessing certain applications data, including prevention of leakage, theft, loss, unauthorized use destruction, distortion, modification (forgery), unauthorized copying, blocking information, etc.

When person takes actions such as hacking your computer, spreading it malicious viruses, which prevents further work computer, password attacks, Application Layer attacks (crashes the server operating system), this list can be continued, however, others can take action to protect themselves from such unauthorized activities actions to protect information, which in this case will be defined as self-protection of information rights. Therefore, by installing the appropriate antivirus you can minimize the application on your computer using passwords, but, unfortunately, does not completely protect the information on your computer system.

In particular, according to official information from National Police of Ukraine in the structure of cybercrime, in Ukraine 65 percentages are exactly fraudulent acts used for committing Internet crime (hacking accounts for 16%, crimes against using payment systems - 13%, 5% - illegal content).

In the first nine months of the year, more than 11 were reported to the cyber police thousands of Internet fraud reports.

However, during this period the Unified Register of Pre-trial Investigations only 966 criminal proceedings have been registered with a qualification for parts 3 and 4 of Art. 190 of the Criminal Code of Ukraine (Fraud), which is 18.4% of the total number of criminal offenses committed with using high information technologies.

However, according to official statistical reporting The National Police of Ukraine, the number of registered during this period pre-trial investigations of criminal offenses committed, skilled in parts 3.4 Article.190 of the Criminal Code of Ukraine, in general significantly decreased from the same period last year (from

[15] Law of Ukraine On the organizational and legal bases of the fight against organized crime from 30/06/1993, http://zakon1.rada.gov. ua/laws/show/3341-12 (consulted on 1.10.2019).

1585 to 966 – 39.1%)[16].

According to experts, this is primarily related to the wrong one qualification of such crimes. In fact, in the vast majority of cases, bodies of pre-trial investigation start criminal proceedings under Part 1 or Part 2 of Art. 190 of the Criminal Code of Ukraine without taking into account the qualifying feature - "Conducted using electronic computing". In general, such a situation is typical of crimes in conditions of non-obviousness, that is, when at the time of commencement of the proceedings no identified the person who committed the crime.

Unfortunately, there is a steady trend of artificial improvement statistics on crime in this category crimes (envisaged by Part 3 and Part 4 of Article 190 of the Criminal Code of Ukraine) in subdivisions of National Police of Ukraine, as they belong to the category of serious crimes.

The problematic issue during the investigation of the such proceedings were disqualified criminal offenses of the specified category in the territorial bodies of the National Police.

Obviously, the problem of information security is one of the most urgent, and the danger of potential threats in the form of IT and banking crime in general and fraud with currencies in particular - the real one that needs a systematic, offensive reaction of the state as well as an improvement of Ukrainian legislation.

5. Conclusion

To summarize, we have to mention that for online banking fraud: there is simply no such thing as a suitable target. Victimization seems to occur because criminals constantly increase their level of different tactics, as a result, they gain the trust of bank clients because people do not understand their new criminal approaches.

Moreover, we have to determine he main factors that effect of the structure to failure of cyberattacks. Accordingly, the main factors are identified: server security mechanism, which stores, coordinates and transmits important company data; the presence of valuable information at the disposal of the company; awareness of working staff with information security issues; use of advanced tools authentication, threat dissemination tools, and more. Also, we should point out that the implementation of these methods of protecting information in the work to reduce the risk of falling victim cyberattacks.

Thus, the last but not least, bank card fraud has significant negative consequences for the stability of the financial system of the state, because it hinders the spread of non-cash payment, which is a recognized priority for the development of the world financial system and also causes significant economic damage to the different subjects of economic processes. That is why actively combating this manifestation of cybercrime is an urgent time requirement that requires the

[16] Shapochka S., *Preventing Fraud Using Computer Networks,* „Internal Security", no. 2, 2013, pp. 63-75.

consolidation of the efforts of banking institutions, law enforcement agencies, NGOs, and of course, bank card users.

Bibliography

1. Leukfeldt, Eric, *Phishing for Suitable Targets in The Netherlands: Routine Activity Theory and Phishing Victimization,* „Cyberpsychology, Behavior, and Social Networking", 17(8), 2014, pp. 551-555.
2. Jansen, J., & Leukfeldt, E.R., *How people help fraudsters steal their money: an analysis of 600 online banking fraud cases,* Workshop on Socio-Technical Aspects in Security and Trust, 2015, pp. 24-31.
3. Yazdanifard, Rashad & Wan Yusoff, Wan Fadzilah & Behora, Alawa & Sade, Abu, *Electronic banking fraud; The need to enhance security and customer trust in online banking*, „International Journal in Advances in Information Sciences and Service Sciences", 3, 2011, pp. 505-509.
4. Shannak, R., *Key Issues in E-Banking Strengths and Weaknesses: The Case of Two Jordanian Banks,* „European Scientific Research", 9, 2013, pp. 239-263.
5. Chavan, J., *Internet Banking - Benefits and Challenges in an Emerging Economy*, „International Journal of Research in Business Management" (IIEBM), 1(1), 2013, pp. 19-26.
6. Bolton, R. & Hand, D., *Statistical fraud detection: A review,* „Statistical Science", 17(3), 2002, pp. 235-255.
7. Omariba, Z., Masese, N. & Wanyembi, G., *Security and Privacy of Electronic Banking,* „IJCSI International Journal of Computer Science Issues", 9(3), 2012, pp. 432-446.
8. Saranya, K. & Gunasri, K., *Challenges in E-Banking,* „International Journal of scientific research and management" (IJSRM), a special issue of journal with no volume or issue number, 2013, pp. 22-27.
9. Bhasin, Madan, *An empirical study of frauds in the banks,* „European Journal of Business and Social Sciences", 4, 2015, pp. 1-12.
10. Chakrabarty, K., *Fraud in the banking sector – causes, concerns and Cures.* The National Conference on Financial Fraud organized by ASSOCHAM, July 26, 2013, New Delhi, India, pp. 1-13. The document is available online at: http://rbi.org.in/scripts/BS_Speeches View.aspx?Id=826 (consulted on 1.10.2019).
11. Vrincianu, M. & Popa, L., *Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests*, „Amfiteatru Economic" no. 12(28), 2010, pp. 388-403.
12. Kovach, S. & Ruggiero, W., *Online Banking Fraud Detection Based on Local and Global Behavior,* The Fifth International Conference on Digital Society, Guadeloupe, France, 2011, pp. 166-171.
13. Shapochka S., *Preventing Fraud Using Computer Networks,* „Internal Security", no. 2, 2013, pp. 63-75.