DOI 10.20544/HORIZONS.A.29.2.21. P20
UDC343.9.024:336.7

CHARACTERISTICS AND TECHNIQUES OF CRIMINAL INVESTIGATION OF COMPUTER FINANCIAL CRIME[1]

Prof. Svetlana Nikoloska, Phd
University „St. Kliment Ohridski“ Bitola, Faculty of security – Skopje
svetlana.nikoloska@uklo.edu.mk

Marija Gjosheva-Krsteski, Phd
Ministry of Interior – Cyber Crime and Digital Forensic Unit
gjoshevamarija@gmail.com

Abstract

Cyber crime is a serious crime that causes not only financial consequences, but also distrust in the business operations of legal entities and distrust of clients towards financial institutions - banks. Forensic research is a procedure of applying tactics of obtaining information, their analysis, assessment of the application of legal measures and technical methods and means in order to clarify and provide evidence, to initiate a procedure. The legislator envisages legal measures and actions, but their application is conditioned by the professional and professional approach of the criminal officers who build and apply appropriate tactics and techniques based on scientific knowledge, but also practical experience. This is the subject of study in this paper in order to obtain indicators on the basis of which strategies will be built for protection of cyber financial data, as well as strengthening the detective function of the police as a competent body for combating this crime.

Key words: Cyber financial crime, forensic research, financial data, detective

[1] professional paper

INTRODUCTION

The computer revolution that intensified during the 1980s and especially in the 1990s, as well as the spread of global computer networks, brought (as with any new technological advancement) new forms of socially unacceptable behavior, which should be appropriately addressed, incriminate. National legislation is redefined on the basis of the recommendations of the international community, in particular the recommendations of international conventions and other legal documents in order to modernize criminal legislation and to improve the criminal investigation of crime that abuses information technology by persons who skillfully use their knowledge and skills in order to carry out illegal, criminal activities in order to achieve their criminal ideas and goals.

The development of information technology, especially in the field of e-commerce and communication, has created a new space for criminal activity of individuals and organized criminal groups.(Urošević, 2009)

The subject of interest of this paper is the phenomenology of crime related to information technology in the field of financial relations and misuse of financial data as well as electronic business communication. The emerging forms of this crime have criminalistic characteristics of both cyber and financial crime, in criminology the new emerging forms of crime are constantly studied in order to find criminal tactics and techniques for its detection, elucidation, evidence and prevention. In order to investigate a certain crime, it is necessary to define it and analyze its criminal characteristics, which distinguishes it from other forms of criminal activity.

In that regard, an analysis will be made of the incriminated cyber financial crimes in the N.Macedonian substantive criminal legislation and the envisaged legal measures and actions in the N.Macedonian procedural legislation.

1. CONCEPT AND APPEARANCES OF CYBER FINANCIAL CRIME

Cyber financial crime is a newer form of crime characterized by the abuse of information technology in achieving criminal goals for gaining criminal financial gain.

Cyber crime includes criminal activities with the misuse of computer data and information from computer systems and databases for the purpose of data theft and identity theft, access to financial accounts in order to initiate unauthorized transactions, fraud in order to obtain funds from other people's accounts of legal entities and individuals. The purpose of this crime is to obtain financial gain through criminal activities aimed at profit, including identity fraud, ransom attacks, e-mail and internet fraud, and attempts to steal a financial account, credit card, or other payment card information.

There is still no generally accepted definition of computer financial crime, as there is no other definition of crime, but the definitions of financial and computer crime would be taken as a starting point for defining this basis. From the definitions of cybercrime it can be taken into account that to commit this crime, the computer is taken as a means of perpetration, but the computer and computer systems are also the object of a criminal attack. (Bequai, 1978) While the definitions of financial crime, especially the newer ones emphasize the role of information technology and the misuse of financial data to achieve financial gain.

The notion of financial crime encompasses a wide range of offenses that are international in nature, related to illegal IT activities, often carried out through the global Internet communication network and have a dominant influence on international banking flows and financial transfers whether official or non-official or other type of communication and misuse of data in communication. (Uljanov, 2018)

The target of a criminal attack are individuals and companies, but also state entities, is the criminal motive is to obtain financial gain, and the manner of criminal action is related to the means of execution, namely computer devices and computer systems and networks through legal tools, but also the creation of programs and schemes in order to abuse the computer databases, where the financial data in the banking system are the most attacked.

Financial offenses destroy or disrupt the commercial efficiency of normative business practices, and the negative consequences are extended to

persons for whom it was not originally intended to suffer damage from the offense, which is the case with computer hacking, insider trading in stock exchange transactions and the like, and that it is a crime in which the perpetrators make cost-benefit analyzes on the basis of which they make the decision whether they can gain high financial benefit from a certain criminal activity, is whether the invested labor can bring them criminal profit. (Gruevska - Drakulevski, 2008).

Based on theoretical analysis and practical experience, cyber financial crime is a criminal act with the abuse of information technology from which computer devices and computer programs can serve as a means of committing crimes, and it can also be the object of a criminal attack, and especially targeted by criminals are computer databases, business communication and correspondence in order to abuse them for financial gain, where fraud and abuse of personal data in financial relations in order to obtain illegal profit in the form of financial assets is crucial.

As a special form of cyber financial crime that is increasingly common in the N. Macedonia, but also in other countries is the crime that is associated with fraud and abuse of electronic communication between business entities. The crime is manifested in a way that monitors the electronic communication, is the criminals access the e-mail addresses, secretly monitor the communication and correspondence and have insight into the business cooperation and concluding contracts. This monitoring of e-mail communication is performed until the moment when an agreement is reached with the business associate for payment on the basis of invoice / for a specific service. At that moment, the fraudsters who have full access to the e-mail address make a change, ie falsify the bank details of the sent invoice in order for it to be paid by the victim to another bank on a fake account. Most often, these fake accounts are opened in different countries of the world and are purposefully used by fraudsters to commit this type of abuse.

In the process of criminalizing crimes in the field of cybercrime, the Macedonian national criminal legislation implements the recommendations of the 2001 Budget Convention on Cybercrime.

1.1. Damage and unauthorized entry into a computer system

Damage and unauthorized entry into a computer system is a crime provided in Article 251 of the Criminal Code of the Republic of Macedonia

(Official Gazette of RM no. 19/04, 114/09 ..... 248/18), it is a complex incrimination which includes multiple criminal behaviors manifested in the deletion, alteration, damage, concealment or otherwise rendering of unusable computer data, a program or device for the maintenance of an information system. The damage that occurs as one of the enforcement actions is in a way a computer sabotage. Namely, this incrimination aims to provide complete protection of computer data and programs. This form appears as a special act in relation to the crime from Article 241 - Damage to other objects (lex specialis derogate legi generali). The modification of a computer data or program is a special modality of the action of committing the criminal act - fraud. Otherwise, changing someone else's automatically processed data is a computer forgery. (Tupancevski and Kiprijanovska, 2008)

Deletion or destruction may occur as a result of the execution, as well as any other way that is unusable of the computer program, data or device for maintenance of the information system. They can also be pre-prepared computer programs in order to cause certain changes or destruction of computer data, and the perpetrators usually do this by creating and launching computer viruses.

The Cyber Crime Convention in Articles 1-6 defines criminal acts of unauthorized access as "acts of unlawful access to all or part of a particular computer system, with intent to misappropriate computer data or otherwise, or in connection with a computer system that is connected to another computer system".

Unauthorized interception actions are defined as "illegal interception actions" using technical means, the transmission of non-public computer data to, from, or within a particular computer system, including electromagnetic emissions from a computer system that supports such computer data.

Damage and unauthorized entry into a computer system according to the criminal acts are a kind of computer theft, computer fraud and the like. Namely, according to how the computer theft is defined, it corresponds to the theft of property data, money of the victims in order to appropriate them, or misuse of computer data in order to redirect financial resources to the name and account of the perpetrator, who uses position to commit the crime, or a job, but what he most often uses is the "exclusivity" of his job, usually a computer scientist is employed and he programs, he makes and corrects mistakes, but he also uses what "there is" no one to control and do programs for diversion of funds, which by the nature of the crime is embezzlement. (Nikoloska, 2015)

1.2. Cyber fraud

One of the typical phenomenological forms of manifestation of financial crime that is gaining alarming proportions in the modern world is cyber fraud. Cyber fraud means any unauthorized entry, change, deletion or concealment of computer data, is any obstruction of the operation of the computer system with the intent to gain illegal property gain for oneself or for someone else. Due to the transnational nature, and above all the fact that the consequences of this crime in the form of property damage can have long-term consequences for the cyber security of financial organizations around the world, and computer fraud as a form of cybercrime allow increased participation of organized crime groups in its execution. (Paunović, 2018).

The criminal offense of Cyber Fraud is incriminated in Article 251-b of the Criminal Code of the Republic of Macedonia (Official Gazette of the Republic of Macedonia No. 19/04, 114/09 ..... 248/18), the legislator provided for criminal proceedings with elements of computer fraud when the perpetrator intentionally obtains illegal property gain for himself or another, by entering false data into a computer or information system, by altering, deleting or concealing computer data, by failing to enter true data, by forging an electronic signature or by otherwise it will cause a false result in electronic data processing.

Cyber fraud is the most common criminal behavior in the world in the field of online market where products are offered and bought online, and it is also paid by electronic transfer of funds for ordered goods. Computer downloaded data for payment card accounts of other citizens, which are mostly from other countries, are most often used as a payment instrument. Experience shows that in the N.Macedonia, this method of payment for expensive goods from abroad is also used, and the perpetrators paid for them by using someone else's payment cards.

1.3 Making and importing computer viruses

Making and importing cyber viruses is a criminal offense provided in Article 251-a (Official Gazette of RM no. 19/04, 114/09 ..... 248/18), which can be committed with two different penalties behaviors of the perpetrator and that one way is the making of cyber viruses, and the other behavior is the introduction of cyber viruses.

The criminal acts refer to:
• Making a cyber virus which is a special computer program that the perpetrator makes for a specific purpose and programs the mode of transmission and what "attack" or damage to be caused, but crime exists if the cyber viruses made in this way are used and specific damage is caused. Downloading, it would mean downloading from another cyber virus as a program in order to use it, is put it in a certain computer network or a specific computer system where it will cause damage or by destroying certain computer data will cause problems in operation, loss of significant data, etc.
• Use, this means that the perpetrator does not program the cyber virus, but only uses it, the previous criminal activities were committed by another perpetrator and certainly have the same criminal purpose.
• The development, download and use of cyber viruses is increasingly becoming an organized criminal activity that causes huge material damage, and more and more perpetrators with their programming and use strive to obtain high criminal returns, the very purpose of criminal activities is "criminal profiting ".
• As more and more companies, due to competition in business, procure and use cyber viruses, liability is also provided for legal entities, when the act is committed by any employes or responsible person, in the name and on behalf of the legal entity.

Cyber crime with elements of making and introducing a computer virus in the scientific and professional literature is also found as computer or logical sabotage. This sabotage involves deleting, damaging, or modifying data, programs, or parts of the operating system, usually by using standard utilities, custom programs, or using techniques such as a logic bomb or virus. Saboteurs have a variety of motives, which can be political, economic, military, official or other private. (Petrovic, 2007).

1.4. Making and using a fake payment card

Making and using a fake payment card is a criminal offense provided in Article 274 - b of the Criminal Code of the Republic of Macedonia (Official Gazette of the Republic of Macedonia No. 19/04, 114/09 ..... 248/18), where it is incriminated making a fake payment card and using itas a real one, using a fake payment card, collecting real bank data for making fake payment cards.

Criminal activity is also criminalized as a qualified form if the crime is committed by an organized criminal group or gang. There is also criminal liability for cases when the crime was committed by an employee or responsible in the legal entity, but in the name and at the expense of the legal entity, parallel liability is provided.

The following actions are envisaged for committing the crime, as follows:

1. Making a fake payment card;
2. Obtaining a fake payment card and
3. Use of a fake payment card.

Making and using fake payment cards is a financial cyber crime that has a wide range of interconnected and conditional criminal activities, so that after the provided data is collected by installing ATM instruments or obtained by downloading data by breaking into the computer data of financial institutions, then fake payment cards are made. This requires equipment, proper knowledge and necessary materials such as "plastics" and magnetic tapes and other materials needed to make fake payment cards. Then, some of the perpetrators themselves or find other people "close to them" to whom they give certain instructions on the use of fake payment cards and instructions on where to "withdraw the money" with those cards. The cards are used at ATMs or post-terminals in the trade network, or with the data from the payment cards, illegal electronic transactions are performed.

2. CRIMINAL INVESTIGATION OF COMPUTER FINANCIAL CRIME

According to the amendments to the Law on Criminal Procedure, the investigation is led by the prosecutor. It has the authority to require the police and other institutions to perform tasks necessary for the investigation and to gather evidence. However, operational work still depends on the capabilities of the police. In principle, the prosecutor should also decide on tasks in the event of a possible overlap between the competencies of the criminal and financial police in each case. The prosecutor has the authority to form investigative teams (Article 50 of the Law on Criminal Procedure), composed of representatives of the relevant institutions (judicial police) for the purposes of investigating a specific case.

Criminal investigation is a process or system that should be applied in the investigation of criminal situations, through the application of measures and actions and a continuous and related process of action and coordination between operational and investigative bodies, in order to fully investigate criminal cases by providing relevant evidence through legal proceedings and procedures according to "case studies" - the method of investigating the criminal case in its entirety, by clarifying and proving all committed crimes, who are the perpetrators and their connection and responsibility for the specific criminal acts committed and their criminal role in the criminal case.

The criminal investigation is related to several phases, as follows: phase of obtaining information - operational information, reporting a cyber crime or reporting by a financial institution or other legal entity for certain suspicious events, followed by the planning phase, the implementation phase specific measures and activities and the phase of submitting a report on the specific criminal situation by filing a criminal complaint or submitting a report to the public prosecutor, and in the case of organized cyber crime and active participation in the investigation process by filing an indictment, but certain measures and activities continue until a final court decision is rendered.

The verification and interpretation of the facts is a process that takes place on a criminal-methodical basis; forensic - psychological and logical plan. The planning enables to discover and clarify the objective - subjective circumstances of the crime and to determine the responsibility of the perpetrator, as well as to determine the further goals of the general and special prevention in a planned, programmed and content rich prophylactic activity of elastic and lasting operative character. (Angeleski M. Gen. quote, p.115)

Cybercrime investigation is related to the application of operational tactical measures, investigative actions and special investigative measures provided by the Law on Criminal Procedure. (Official Gazette of RM no. 115/10.)

The measures and actions are applied after receiving or having general suspicions of cyber crime or general suspicions of criminal activity of certain persons who are suspicious in the way of communication, the way of behavior, and especially with the fact that young people are involved who want to short period to acquire financial resources.

As immediate goals of the criminal investigation carried out through operational-tactical work of the police are:

• Realization of operational penetration among the perpetrators;

• Determining and providing facts about the criminal activity of operational and legal
significance;
• Raising the suspicion from the level of grounds for suspicion to the level of reasonable
suspicion, which would enable the initiation of criminal prosecution against the probable
perpetrators and
• Timely prevention of suspicious transactions or classic illegal actions that would cause
greater financial damage to the State or to financial institutions and individuals. (Batkovski T.
Gen. quote p. 104).

When investigating cyber crimes, operatives plan and implement simple and complex operational combinations.Simple criminal combinations are those when only one type of measures and actions are planned and undertaken, which is not typical for this crime, for cyber crime and its complete detection, elucidation and proving, combined or complex criminal combinations are planned and implemented by applying more operational-tactical measures, investigative actions and special investigative measures.

In recent years, special investigative measures are often applied in order to obtain relevant data and knowledge about the criminal activity of organized criminal groups that usually commit a series of crimes in several places and for a long period of time criminalize, and to catch perpetrators and at the time of the commission of the crime.Immediate arrest at the moment of committing a criminal activity is possible only by applying special investigative measures, which is the most common application in the case of more massive "ATM thefts" or "use of fake payment cards" as a criminal end to criminal security activities of data for making fake payment cards.

Criminal combinations are made by applying several measures and actions (complex criminal combinations) and they are planned and implemented most often: identification of persons; inspection and search of vehicles, persons and luggage; insight into business documentation; examination and search of persons; search of an apartment and business premises; computers and computer data are confiscated; Bank checks are carried out and activities are undertaken to freeze financial accounts, freeze movable and immovable property, all in order

to enable full clarification of the criminal situation on the principle from information to realization and confiscation of criminally obtained proceeds.

Depending on the type and nature of the cyber incident, appropriate measures are taken at the time when the perpetrator commits the crime or when he is connected to a computer and there are suspicions that something "criminal" is related to the rest of the criminal group on the computer network, to provide evidence, it is necessary to "catch when it is on" or "on line".

In the case of an online criminal attack, several situations are possible: that the perpetrator is connected to the network and there is a real chance that the tactical "entry into the home" will turn on the computer and the perpetrator is logged in. time for destruction of digital evidence (with whom it is in contact, messages between them, e-mail, etc.) ".

The results of the forensic investigation of the cyber incident should be summarized and provided with answers to the main forensic questions. The investigation of cyber crime and other abuses of information systems and networks can often end without results, such as catching the perpetrator, prosecuting him and sanctioning him, and this happens for several reasons:

- Loss of traces due to the long time since the incident and no evidence;
- Incomplete login or not at all;
- The costs of the investigation are higher than the damage caused as a result of the incident

and it is not profitable to continue the investigation;

- Large space for hiding the perpetrator (Internet), and the incident happened only once, with

little or no evidence;

- The incident is not completely determined, it is not clear whether it is or is not a security

incident;

- The perpetrator cannot be indisputably pointed out;
- There is not enough evidence to prove the case irrefutably;
- Closing the investigation, etc.

Computer data are temporarily confiscated, such as data stored in a computer and similar devices for automatic or electronic data processing, devices used for data collection and transmission, data carriers and subscriber information available to the service provider. With a special decision of the judge in the preliminary procedure, and upon the proposal of the public

prosecutor, the protection and storage of the computer data can be determined, while it is necessary, and for a maximum of 6 months, then they are returned unless they are involved in committing computer crimes, specified in the law. (Criminal procedure law, a.198).

3. VOLUME, STRUCTURE AND DYNAMICS OF CYBER FINANCIAL CRIMES

In 2019, the crime of computer crime increased by 65.7%, is 174 (105) crimes were registered, for which 124 perpetrators were criminally reported. It is characteristic that by committing these acts, material damage of 42.6 million denars was inflicted on individuals and legal entities, which compared to the previous year when the caused material damage amounted to 11.2 million denars, is an increase of 280%. The increase in intelligence activity is primarily due to the large number of detected content on Internet portals and social media that promote or incite hatred, discrimination or violence against individuals or groups based on ethnic, religious and political affiliation, as well as the increasing number of cases of misuse of personal data. In this part, 29 criminal offenses of endangering security, 27 criminal offenses of spreading racist and xenophobic material through a computer system were registered, as well as 19 criminal offenses - misuse of personal data.

According to the observations made in the area of cyber crime, in 2019, in addition to the above forms and modes of execution of the crimes, are characteristic: In the area of payment cards compared to the previous year, crimes increased by 28%, is 73 crimes were detected 65 criminal offenses "damaging and unauthorized entry into a computer system", as well as eight criminal offenses "making and using a fake payment card". Most often, these are previously committed thefts of debit and credit electronic cards from citizens, from which the perpetrators later withdrew cash from ATMs or electronic transactions were performed online.

In the area of cyber fraud, 12 crimes were registered, and are characterized by a significantly more complex manner of execution, as well as causing great material damage compared to other crimes in this area, which this year amounts to 36.3 million denars or 85 , 2% of the total material damage. In internet scams, the most common are false advertisements for buying and selling on internet portals, as well as interception of e-mail communication between private

companies in order to defraud, direct and pay to another bank account. (Years report of MOI, 2019).

In 2020, the crimes in the field of cybercrime decreased by 8.6%, ie 160 crimes were registered, for which 88 perpetrators were criminally reported. These crimes caused material damage of 12.6 million denars, which is significantly reduced compared to 2019 when it was estimated at 42.6 million denars. This year, 103 criminal acts were registered, is 85 criminal acts "damaging and unauthorized entry into a computer system", and 18 criminal acts "making and using a fake payment card".

Particularly emphasized are the activities for detection and elucidation of the conditions and phenomena related to the spread of racist and xenophobic material, whereby 28 (29) criminal acts "endangering security" and 16 (27) criminal acts "spreading racist and xenophobic" were detected. information through an information system ".(Years report of MOI, 2020).

4. MANNER OF COMMITTING CRIMES IN THE FIELD OF INTERNET FRAUD

Recently, internet frauds have become more frequent in the Republic of N.Macedonia, where the most frequent victims are Macedonian citizens and legal entities from the country. Frauds are most often committed by the fact that the e-mail address with which the Macedonian legal entity communicates with its associates from the country and abroad and through which business deals and cash payments are negotiated is misused, ie the e-mail address and password are stolen and the content of it is under the control of fraudsters. That is, after the fraudsters access the e-mail address, they secretly monitor the e-mail correspondence and thus have insight into business collaborations and agreements.

This monitoring of e-mail communication is performed until the moment when an agreement is reached with the business associate for payment on the basis of invoice / proforma invoice for a specific service. At that moment, the fraudsters who have full access to the e-mail address make a change, is falsify the bank details of the sent invoice in order for it to be paid by the victim to another bank on a fake account. Most often, these fake accounts are opened in different countries of the world and are purposefully used by fraudsters to commit this type of abuse.

Due to the complex way of investigation that includes international organizations for police cooperation and various legal regulations in the countries where the "stolen" funds flow, the best way to fight this type of crime is the prevention and high level of awareness when using the Internet in business communication.

It is necessary for legal entities and individuals to protect themselves from this type of fraud. The e-mail addresses that legal entities use for business cooperation should be used as professionally as possible and by a limited number of employees in the company, e-mail addresses to contain complex characters and to change them over a period of time, if possible, for business purposes to avoid the use of commercial e-mail services and to replace them with professional IT companies that offer such services and quality guarantees It is obligatory to make a telephone or other type of confirmation with the business associate for the agreed invoices / proforma invoices, especially if there is a change in the bank data where the funds are to be paid, the suspicions of fraud should be reported to the responsible The bank where the legal entity is a client in order to be able to prevent the execution (processing) of the transaction in a timely manner.

CONCLUSION

What distinguishes this crime are the means of execution, and they are electronic devices, computer data, computer systems which, depending on the criminal situation, can be a means of execution, but also an object of criminal attack, but the sphere of criminal activity is financial relations, electronic commerce, electronic communication, etc.

Cyber financial crime is also found in descriptive definitions of financial crime. According to the definition of the Council of Ministers of the Council of Europe in Recommendation no. (81) 12, in addition to the numerous manifestations and forms of economic-financial crime, cyber crime is also mentioned, but also other forms that can be committed with the abuse of information technology and have the characteristics of both financial and computer crime such as are business relationship abuse and fraud. (Nikoloska, 2015).

This crime has its own important criminalistic characteristics that arise from computer crime that the perpetrator can act from one point on Planet Earth, and the consequences occur at the other end of the world. The perpetrator and the victim do not know each other personally. This would mean that the possibilities of information technology and communication (as a means of execution) allow the perpetrators to act criminally in a huge space or globally, and they adjust the time depending on the criminal idea and the achievement of the criminal goals. This crime is sophisticated, difficult to detect, and the process of clarifying and providing evidence is complex, professional and with a serious professional and team approach and knowledge of electronic techniques and tools for analyzing and extracting electronic evidence crucial for initiating criminal proceedings against perpetrators and sanctioning them.

The suppression of cyber financial crime nationally, and especially internationally, is a prerequisite for criminalizing criminal offenses in national legislation and procedural actions to provide electronic evidence-based procedural procedures to fully investigate a computer incident with elements of cyber financial crime.

REFERENCES

August Bequai, *Computer crime*, Lexington, 1978;
Eilam, E. (2011) Reversing: *Secrets of Reverse Engineering*. Hoboken: John Wiley & Sons;
Gruevska - Drakulevski A. (2008), *Recidivism in economic crime in the Republic of Macedonia*, MRCPC, no. 2 - 3, Skopje, 2008;
Hadnagy, C. (2011) *Social Engineering: The Art of Human Hacking*. Indianopolis: Wiley Publishing, Inc.;
Nikoloska. S (2015) *Methodology of general crime research*. 978-608-4532-34-7., Faculty of Security - Skopje, Skopje, 2015;
Mitnick, K.D., Simon, W.L. (2011) *The Art of Deception, Hoboken*: John Wiley & Sons.
Paunović N., (2018), *Criminal offense of computer fraud as a form of financial crime - criminalistic aspect*, Proceedings of the scientific conference FINANCIAL CRIME 7.- 8. September, Zrenjanin, Serbia;
Petrovik.S, (2007), *Police Informatics, Criminalistic* - Police Academy, Belgrade;
Tupancevski.N and Kiprijanovska D.,(2008), *Fundamentals of the Macedonian Information Criminal Law*, MRCPK no. 2 - 3, Skopje;
Uljanov S., (2018) *INTERPOL's typology of financial crime*, Proceedings of the scientific conference FINANCIAL CRIME 7.- 8. September, Zrenjanin, Serbia;
Urošević, V. (2009), *"Nigerian fraud" in the Republic of Serbia*. Security, 3, 145-156;
https://mvr.gov.mk/Upload/Editor_Upload/%D0%9E%D0%9A%D0%A0%D0%90/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202019.pdf, (YearsReport MOI 2019);
https://mvr.gov.mk/Upload/Editor_Upload/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202020.pdf, (YearsReport MOI2021).