TALLINN UNIVERSITY OF TECHNOLOGY

School of Business and Governance

Department of Law

Igor Stulov

INVESTIGATION OF INTERNET FRAUD IN THE PROSECUTION PROCESS

Master's thesis

Programme HAJM08/15

Supervisor: Aleksandr Popov, MA

Co-supervisor: Pawan Kumar Dutt, MA

Tallinn 2018

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not previously been presented for grading.
The document length is 20708 words from the introduction to the end of summary.

Igor Stulov ……………………………
(signature, date)

Student code: 152717HAJM
Student e-mail address: igor.stulov@gmail.com

Supervisor: Aleksandr Popov, MA:
The paper conforms to requirements in force

……………………………………………
(signature, date)

Co-supervisor: Pawan Kumar Dutt, MA:
The paper conforms to requirements in force

……………………………………………
(signature, date)

Chairman of the Defence Committee: /to be added only for graduation theses/
Permitted to the defence

…………………………………
(name, signature, date)

TABLE OF CONTENTS

LÜHIKOKKUVÕTTE EESTI KEELES

Tänapäeval üks levinumaid kuritegude liike, mida pannakse toime interneti teel on kelmus. Kelmus on üles ehitatud pettusele ja usalduse kuritarvitamisele. Internetikelmuse on suhteliselt lihtne toime panna, kuid selle uurimine on keeruline, vajab kõrget IT alast pädevust, ja suuri uurimisasutuse ressursse.

Käesoleva lõputöö eesmärk on kokku viia teoreetilised ja praktilised internetikelmuste uurimise ja tõendite kogumise meetodid, mis vastavad käesoleva aja tehnoloogiate arengu tasemele. Selle saavutamiseks on püstitatud järgnevad uurimiseesmärgid:

Uurida ja analüüsida internetikelmuse teaduslikud kontseptsioonid.

Välja tuua asjaolusid, mis vajavad kindlaks tegemist internetikelmuse uurimise käigus.

Selgitada välja uurimisasutuse ja menetluse seisukohalt vajaliku teabe omava isiku efektiivse koostoime võimalusi internetikelmuse uurimisel.

Selgitada välja uurimise korraldamise ja tagamise meetodite kitsaskohti internetikelmuse uurimise puhul.

Töö teoreetiline ja praktiline tähtsus seisneb internetipettuste uurimise meetodite väljatöötamise ja rakendamise teoreetiliste ja praktiliste aspektide arendamises. Töös sisalduvate eelduste ja järelduste eesmärk on süvendada, üldistada ja täpsustada organisatsioonilisi ja taktikalisi omadusi nendes kriminaalasjades, mis saavad olla kasulikud Internetis levinud pettusel ja usalduse kuritarvitamisel üles ehitatud kuritegude menetlemisel ning muude kõrgete infotehnoloogiaalaste kuritegude menetlemisel, et parandada uurimisasutuste õiguskaitsealase tegevuse efektiivsust.

Selle kategooria kuritegude toimepanemisel jälgi moodustumise mehhanismi eripära on see, et virtuaalsete teede moodustamine põhineb spetsiifilisel elektroonilisel digitaalsel kaardistamisel, mis esineb arvutisüsteemis ja (või) virtuaalses ruumis. Küberkuritegevuse toimepanemise koha

tuvastamine on võimatu, kui pole loodud keskkonda kuriteo toimepanemiseks, mis määrab kindlaks küberruumi süsteem.

Küberruumis toime pandud kuritegude uurimiseks on vaja nii tehnilisi kui ka teoreetilisi teadmisi. Seepärast on kohtuekspertiisina vaja välja töötada ühtne küberruumi mõiste. Küberruum on erinevate tasandite süsteemide koostoime ala, sealhulgas järgmised elemendid: arvuti, arvutisüsteemid, võrgud (nii globaalsed kui ka kohalikud), kasutajate arvutiprogrammid, samuti loetletud elementide ringlevad andmed. Interneti-pettuse edukas uurimine sõltub paljudel juhtudel juurdluse alguses uurija käsutuses olevast esialgsest teabest. Üks sellist teavet võib pidada kohtuekspertiisi klassifikatsiooniks. Kuritegude kuritegude kuritegevuse liigitamine on suunatud ka aktiivse praktilisse rakendamisse uurimistööde käigus, aitab teadvustada uuritavate sündmuste sisulist olemust, kriminaalsete meetodite pädevat ehitamist, valimist ja rakendamist teatud liiki pettusele.

Töö käigus tehtud teaduslikud uuringud võimaldasid teha mitmeid järeldusi.

1. Interneti-pettustel on traditsioonilise pettusega võrreldes mitmeid erinevusi. Need erinevused määravad selle kuriteo uurimise eripära. Eelkõige ilmnevad sellised tunnused operatiivtegevuse ja jälitustoimingute teostamisel.

2. Interneti-pettuste uurimisel toimivate otsingutegevuste ja jälitustoimingute keerukust teeb asjaolu, et osa nende teostamisel hangitud informatsioonist on saadud virtuaalsetest andmetest (ohvri või kuriteo arvutist, kohalik server, Internet jne)

3. Uuritud materjali põhjal töö kolmandas peatükkis tehakse uurijatele soovitusi teatavate operatiiv- ja jälitusmeetmete ning uurimistoimingute teostamiseks, mis on Interneti-pettuse uurimisel on eriti olulised ja keerukad.

ABSTRACT

Among the crimes known to date, committed in the Internet, a particular danger is the Internet fraud. Due to its high latency, as well as difficulties in identifying and investigating, this crime requires a comprehensive scientific study

The purpose of the study is to examine theoretical and practical issues of the methodology for investigating Internet fraud, which corresponds to the current level of development of high information technology.

To achieve this goal, the following main objectives are formulated:

1. To study and analyze the scientific concepts of the concept of Internet fraud;

2. To determine the circumstances to be determined in the investigation of fraud in the Internet;

3. Identify and develop the most effective forms of interaction of the investigator with persons with special knowledge in the investigation of fraud in the Internet.

4. To consider and analyze the problems of organizing and ensuring the investigation of Internet fraud.

The methodological basis of the study is the dialectical theory of knowledge, formal logic, forensic methodology and general theoretical concepts of criminalistics. The general scientific methods of cognition (analysis, synthesis, statistical method), as well as methods of other sciences, in particular, the basis of the theory of information security, were used in the work.

Keywords: Internet fraud, Europol, investigation, evidence, Cyber-crime, Law enforcement

INTRODUCTION

For the current society, an acute problem is security in general, and information security in particular. The rapid formation of information technologies in the managerial, commercial, industrial, banking and other spheres of society requires a qualitative growth in the level of information security. Improving computer technology and technology, scientific and technological progress, the emergence of global information networks has identified a new type of socially dangerous behavior - crimes in the field of computer information.

Among the crimes known to date, committed in the Internet, a particular danger is the Internet fraud. Due to its high latency, as well as difficulties in identifying and investigating, this crime requires comprehensive scientific research.

The growth of the number of online stores, the creation of systems for the provision of banking services through a global network, the development of payment systems contributes to the fact that more and more people trust in non-cash payments, forgetting that even in virtual economies, criminal elements operate.

Despite the large number of publications devoted to the investigation of crimes related to the use of computer equipment, which have appeared recently, the questions of the methodology for investigating Internet fraud were practically not considered. Most of the works published today on the topic of crimes in the sphere of high technologies, if they mention fraud, then casually, often stopping at the study of crimes such as unauthorized access to computer information.

At the same time, there is an objective need to develop comprehensive guidelines to improve the effectiveness of the participants in the preliminary investigation in identifying and investigating Internet fraud.

Thus, the relevance of the thesis is due, on the one hand, to the high practical importance, and on the other hand, to the insufficient scientific elaboration of the methods of investigating fraud in the Internet.

The object of work is the criminalistics characteristics of Internet fraud, as well as the specifics of the investigation of this type of crime.

The subject of the work are the patterns of the formation of investigation techniques, as well as the use of special knowledge in the field of computer information and high technologies in the investigation of various types of fraud using the global Internet.

Author states the hypothesis, that currently existing methods of gathering evidence in the prosecution process are insufficient for the area of internet crimes and internet fraud in particular. To prove or refute the hypothesis in current paper the study is made to gather data, examine theoretical and practical issues of the methodology for investigating Internet fraud. Author's further goal is to find and fill the gaps in methodology of investigating internet fraud.

To achieve this goal, the following main objectives are formulated:

1. To study and analyze the scientific concepts of the concept of Internet fraud;

2. Determine the circumstances to be determined in the investigation of Internet fraud;

3. To consider and analyze the problems of organizing and ensuring the investigation of Internet fraud.

The methodological basis of the study is the dialectical theory of knowledge, formal logic, forensic methodology and general theoretical concepts of criminalistics. The general scientific methods of cognition (analysis, synthesis, statistical method), as well as methods of other sciences, in particular, the basis of the theory of information security, were used in the work. Therefore author is using a qualitative research method in the paper that is in some cases supported by numerical data taken from other researches.

Theoretical and practical significance of the research. Theoretical significance of the research is determined by the contribution to the development of theoretical and practical aspects of the development and implementation of methods for investigating fraud on the Internet. The provisions and conclusions contained in the work are aimed at deepening, generalizing and concretizing organizational and tactical features in these criminal cases. They can be useful for further research related to the investigation of mercenary crimes committed on the Internet by fraud and abuse of confidence, as well as other crimes in the field of high information technology.

The practical significance of the research is that the scientific provisions and practical recommendations worked out in the thesis are designed to improve the effectiveness of the law enforcement activities of the preliminary investigation bodies.

Within current paper author focuses on internet fraud, therefore cyber-crimes against intellectual property, authors rights violation etc are not observed in current paper, because the compositions of perpetration in those cases are significantly different. For example in Estonia violation of authors rights is mostly regulated by Autoriõiguse seadus (Copyright Act), and also international and European conventions on copyright, and perpetrations connected to internet fraud are described by Karistusseadustik (Penal Code). Therefore copyright and intellectual property right violation investigation methods will not be included in the paper, and cases relevant to those perpetration will be observed only in case of need. Also author does not focus on extradition and cross-border arrests of cyber-criminals, because it is a wide topic for multiple researches on its own.

Structure. The thesis consists of an introduction, three chapters, a conclusion and a list of used literature.

The first chapter is devoted to the forensic characterization of fraud in general, and especially, fraud in the Internet. In particular, on the basis of the studied approaches to the solution of the problem of the content of the concept of forensic characteristics of fraud, five main elements were identified that were taken as a basis for further disclosing the criminalistics characteristics of Internet fraud.

The second chapter is devoted to the study of the circumstances to be determined in the investigation of fraud in the Internet.

The third chapter is devoted to the general issues of organizing investigative activities in the course of investigations.

CHAPTER 1. CRIMINALISTIC CHARACTERISTICS OF INTERNET FRAUD

1.1 DEFINITION OF THE CONCEPT OF INTERNET FRAUD

Internet today except topical and useful information contains potentially harmful and illegal information, which are fertile soil for the deployment of activity. The global network is characterized by the simplicity and cheapness of formations: every person, having a computer and connecting to the Internet through the provider, can create a personal website or an account on a social network, and establish the owner in most cases impossible. A networked environment capable of influencing personal characteristics people. The virtual world provides additional freedom of action and expression of the lei, emotions and feelings, but at the same time can easily draw into the communication of marginal groups. Even with a shallow search, one can find sites where Satanism is positively assessed, drugs are distributed, suicides are supported.[1] Young people with unstable psychic can actively take in the propagandized views and transfer them to their own everyday life. For young people, the virtual environment sometimes seems even more than real. Young people can trust a complete stranger (anonymous user of the World Wide Web), but may not take into account the words not only their friends, but relatives and friends.

The development of forensic science is now characterized by intensive enrichment with thematically integrated concepts and definitions. This trend is an indicator not only of the expansion of the volume of forensic knowledge, but also of their qualitative change, which is the space in which forensic definitions and concepts are developed by which forensic science operates and the number of forensic interpretations of dpefinitions used in the scientific-natural language is increasing. Performing a communicative and cognitive function, the definition (concept, term) expresses a certain category of information about the object of cognition and is understandable for

[1] Riordan J., The Liability of Internet Intermediaries, Oxford University Press, Oxford, 2016, par 11.11-11.96

persons who do not possess narrowly forensic knowledge. The language of science (terminology) should be distinguished by exceptional accuracy, certainty, uniqueness of the terms used and terms. In this connection, the introduction of new concepts and definitions into criminalistics can be achieved at the expense of real results of scientific knowledge on the basis of interconnection and interpenetration.[2]

The aforementioned proposition is valid also with reference to the concepts of «cybercrime» and «cyberspace», which are currently used quite widely in connection with the information and telecommunications breakthrough that occurred in the 21st century and have become an integral part of all spheres of human life.[3] Today, in the systems of remote banking services via electronic channels, electronic media, technical devices, computer programs, money is transferred, and various goods are bought and sold. Thus, according to the United Nations, in 2016 at least 2.5 billion people or more than one third of the total population of the world had access to the Internet, and by 2018 the capacity of mobile broadband Internet will be able to use at least 75% of the total population planet.[4]

With the development of information technology, the concept of «computer» becomes commonplace. Currently, almost all gadgets have access to the Internet. With the development of 3G and 4G networks, mobile phones connect to the global network using UMTS (third generation network) technology or HSPDA (fourth generation network) and are almost as fast as the Internet connection through a trivial computer, and in the future, will surpass it by technical characteristics and parameters.

With the increasing statistics of users, the computer increases as the number of trusting consumers who are not able to abandon tempting offers, and those who use the Internet to commit unlawful acts. Computer and telecommunication systems offer not only unique opportunities to meet the widest human needs in all spheres of its life and the functioning of the state, but also create favorable conditions for various kinds of malicious acts. There are people and organized groups,

[2] Chang, J.J.S., An analysis of advance fee fraud on the internet. Journal of Financial Crime, Vol. 15 Issue: 1, pp.71-81.

[3] Chiemeke, S. C., Evwiekpaefe, A. E., The Adoption of Internet Banking in Nigeria: An Empirical Investigation. Journal of Internet Banking and Commerce, 2006, Vol 11 (3).

[4] UN report from 15.09.2016

professionally doing their business in high-tech fraud and illegally gaining huge profits.[5] The incomes of such criminal users range from 1,000 to 15 - 20 million dollars a month.

The scale and structure of cybercrime vary considerably from country to country and depends primarily on the nature and level of development of information technology, the extent to which the Internet is used, the use of electronic services and e-commerce, etc. In the United States, the structure of cybercrime is as follows. According to the proven data, embezzlement of money from electronic accounts is 44%; software damage - 16%; as many - Theft of classified information; falsification of information - 12%; the order of services for someone else's account -10%.[6]

1.2 Common schemes of internet fraud

Fraud is the creation of an incorrect understanding of the actual circumstances of the dogmatics of penalty law, which results in the victim's mistake. Logically, it is logical to conclude that it is not possible to deceive a computer, because on the contrary to popular science fiction, the computer system has no consciousness and imagination; the computer cannot be faulty.[7] The term «Internet fraud» is applicable in general to fraudulent acts of any kind, where one or more Internet elements are used - such as chat rooms, e-mail, message boards or websites - to attract potential victims, fraudulent transactions or to transfer proceeds from fraudulent activities in financial institutions or other persons involved in such fraud.

In this regard, the most common schemes of fraud in the Internet include the following:

- «Pump & dump» scheme is a kind of market manipulation, consisting in extracting profit from the sale of securities, the demand for which was artificially generated. Initially, there is an increased demand for certain securities, then their sale at inflated prices. After making such

[5] Grazioli S., Jarvenpaa S.L., Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers, IEEE Transactions on systems, man and cybernetics, 2000, Vol. 30:4, July 2000, p 395- 410.

[6] U.S. consumers and cyber crime – Statistics & Facts 2017

[7] Elkind, E., Varavastane süütegu Interneti keskkonnas: selle piiritlemise probleemid Eesti karistusõiguses. Juridica, 2008, No. 2008/5, p 333-337.

manipulations, the price on the market returns to its initial level, and ordinary investors are at a loss;[8]

- The Pyramid Schemes scheme when investing money using Internet technology completely repeats the classical financial pyramid. The investor receives a profit solely by involving new investors in the game;[9]
- The «risk-free» Fraud scheme or «investment scheme» consists in spreading through the Internet investment proposals with low risk and high profit levels. For example, investing in allegedly highly liquid securities of unknown companies. Among such schemes there are also sites offering participation in some business for a one-time payment;[10]
- fraud using banks (Prime Bank Fraud) are that scammers, under the guise of the names and guarantees of well-known and respectable financial institutions, offer investors the investment of money in unsecured obligations with unrealistic rates of return;
- Phishing (originally comes from the word "fishing") is a type of Internet fraud, the purpose of which is to get data stored on a plastic card. Attackers send emails on behalf of banks or payment systems. The user is invited to visit the site, which is an exact copy of this site of the bank. For the further possibility to use the plastic card, the owner is asked to indicate the pin-code and personal data contained on the card. Subsequently, these data are used to make a fake plastic card and cashing out money[11];
- Internet begging. On the Internet, there may be announcements, for example, from a charitable organization asking for material assistance to sick children. Attackers create a site-understudy, which is an exact copy of the present and change the details for transferring money;
- Auctions and retailing online. A distinctive feature of this type of fraud is the low price for a certain product and the absence of the actual address or phone of the seller. In this case, a counterfeit, poor-quality product or money of buyers is simply given, and the goods are not delivered. It is especially complicated to find grounds for a claim of perpetration it the sellable

[8] See more about Pump And Dump Schemes at: https://www.investopedia.com/terms/p/pumpanddump.asp

[9] A good example of Pyramid scheme is MMM, that have originally emerged in Russia multiple times during the 90's and then repeated in different countries around the globe. The scheme recently emerged as an online investment service in Baltic States in 2012.

[10] Example of risk-free scheme is realtranslatejobs.com website, promising the possibility to earn up to 500 USD per day, by working as a translator from a home office after paying the registration fee, and promising 100% money back guarantee for 60 days. Currently this website is visible, but any payment opportunities to its accounts are suspended.

[11] Moreno-Fernandez, M.M., Blanco F., Garaizar P., Matute H., Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud, University of Deusto, Elsevier Computers in Human Behavior, Vol 69, April 2017, p 421-436

goods are not physical but informational content, because it is hard to give legal evaluation to the accordance of content to the expectations of the victim.[12]

- Identity theft. A characteristic feature of Identity Theft is the transmission, access, or use of personal data of another person without his permission, in order to create a knowingly incorrect impression of his appearance as a second person. Identity theft distinctions are relevant only to the use of personal data and the appearance of another person for the purpose of knowingly creating an incorrect image, insofar as such activities may also be included in acts of defamation or offense.[13]

Deception in the conduct of computer fraud is the deliberately incorrect design of computer programs, unauthorized influence on the information process or the improper use of the data bank, the use of incomplete or defective, distorted programs in order to obtain someone else's property or the right to it.

The main problems, as follows from the analysis of forensic investigation, arise in connection with the qualification of fraudulent activities on the Internet. An urgent issue is the need for additional qualification of fraudulent activities committed on the Internet.

Fraud is constantly evolving, acquiring new forms, more adapted to the changing conditions of social and economic life. The most sophisticated of its forms is Internet fraud. Its scope only year 2016 increased by almost a third, in money terms this means growth of almost three times. The cases of thefts in online stores began to occur twice as often.[14]

Of course, security on the Internet also does not stand still: the methods of its provision are being improved day by day. But at the same time, fraudulent schemes are developing, becoming more sophisticated, cunning and confusing. For example, in New York, police detained a group of intruders who abducted personal data of clients. They did this, finding work in various restaurants

[12] Helberger, N., Loos, M. B. M., Guibault, L., Mak, C., Pessers L., Digital Content Contracts for Consumers: Digital Content Contracts for Consumers. Journal of Consumer Policy, 2012, Vol. 36, No. 1, p 3.
[13] Nimmo, M., Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis, Juridica 2017/10, 2017, p 710-717
[14] U.S. consumers and cyber crime – Statistics & Facts 2017, see figures at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

and shops. Using the information obtained, the fraudsters issued credit cards and then purchased the goods. Then the production came true in a number of other countries.[15]

Fighting fraud is a very difficult economic, psychological, legal and technical task. Paradoxically, this problem reflects, on the one hand, the existence of a decline and «shadows» in the economy, and on the other hand it is the fruit of its active development, in particular, the expansion of the scale of business in the «World Wide Web».

For the most part, Internet fraud continues the tradition and principles of traditional fraud. However, it has some specific characteristics:

- It differs internationally;
- Most often it is latent (that is, not registered and not punished);
- Frontmen (physical and legal) are often used;
- The chain of a criminal act is very complex, consists of a large number of links, and each of the participants of any stage is only «partly» guilty.

Usually scammers use in their activities, stolen data about the cards, websites or accounts of other people. For example, about a quarter of transactions through electronic payment systems are rejected today due to the inability to confirm confidential data. Separate attention deserves and online shopping. The cases of fraud with their participation occur ten times more often than, for example, fraud with plastic cards, which buyers pay off-line.[16]

This situation leads to the fact that many people are simply afraid to pay «plastic» on the Internet. For example, 20% of users never complete the transactions that they started before they are completed, because they refuse to enter personal data. It is established that about a third of the cards that «lit up» in payment systems are fraudulent. The conversion reaches a value of 2-3%. Many visitors to online stores do not go there to buy any goods or services, but to obtain confidential information from other customers.

[15] Pratt T. C., Holtfreter K., Reisig M. D., Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory, Journal of Research in Crime and Delinquency, vol. 47, 2010. p 267-296.
[16] Chua, C.E.H., Wareham J., Fighting Internet auction fraud: an assessment and proposal. IEEE Xplore: Computer. Vol. 37, Issue. 10, Oct. 2004. p 31-37.

A special role in the situation is played by the latent nature of fraud, as well as the prevalence of transactions in small amounts. Representatives of online stores say that about 25% of attempts to make payment - this is the action of Internet scammers. Transactions in this case, as a rule, are rejected due to the fact that the user cannot pass primary or secondary authentication (his card has expired or its number is entered incorrectly a large number of times). And the data provided by VISA make us think: more than 47% of cards presented for various operations belong to intruders. However, this figure has no official confirmation.[17]

The problem is aggravated by the fact that it is not possible to solve it by the forces of only one state. Coordination of actions at the international level is necessary in the fight against this transnational evil. In the Manual on the Prevention and Control of Internet-Related Crime for Members of the United Nations, criminal encroachments in cyberspace have been recognized as a global international problem. Similar provisions include other international normative legal acts: the Council of Europe Convention on Cybercrime, the Bangkok Declaration, the Okinawa Charter for the Global Information Society.

Let us also emphasize that until now the world community has not developed a single terminology and a unified approach to the phenomenon and concept of cybercrime, which is used along with the notion of computer crime.

An attempt to explain the essence of the concept of cybercrime was undertaken by the United Nations Congress on the Prevention of Crime and the Treatment of Offenders. According to its resolution, «cybercrime is any crime that can be committed by means of a computer system or network, within a computer system or network, or against a computer system or network». In other words, any illegal act committed in an electronic environment can be referred to cybercrime. [18]

In 2013, the United Nations Office to Combat Drug Trafficking published a report «A Comprehensive Study on the Problem of Cybercrime and Response from Member States, the International Community and the Private Sector»[19] in which the notion of «cybercrime» was dependent on the context and purpose of the term.

[17] Taylor R. W., Digital Crime and Digital Terrorism, 3rd edition, 2015, p 40-62

[18] Albert M. R., E-buyer beware: why online auction fraud should be regulated, American Business Law Journal, p 575-644

[19] Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. Expert Group to Conduct a Comprehensive Study on Cybercrime Vienna, 25-28 February 2013

In addition, as the report emphasizes, the list of computer crimes includes not only crimes against confidentiality, integrity and accessibility of data, but also any acts aimed at unlawfully extracting profits, content-crimes and other unlawful acts in cyberspace. Moreover, as the authors of the report note, «there is no need to create a universal definition of cybercrime, as, for example, for the purposes of international cooperation in the investigation of crimes, it is much more important to harmonize the norms relating to the collection and provision of electronic evidence. This need is not limited to some artificial term «cybercrime», because electronic media and electronic communications can contain information pertaining to any kind of crimes committed both in cyberspace and outside it.

The authors of the «model law» on cybercrime of the International Telecommunication Union (2009), which relate them to unlawful acts committed in cyberspace, and the subject of attacks are: «computers, computer systems, networks, their computer programs, computer Data, content data, traffic, and users».[20]

At present, the official legislative definition of the term «cyberspace» at the international level is not accepted, however, as is the definition of Internet fraud.

[20] Pratt (2010), *supra*

CHAPTER 2. FORENSIC CHARACTERISTICS OF INTERNET FRAUD

2.1. General provisions on forensic characteristics of Internet fraud

Private forensic techniques are the ultimate «product» of forensic science, which comes into the service of investigative practice. In their content, on the basis of the provisions and conclusions of the general and individual forensic theories, criminalistics recommendations for identifying, uncovering, investigating and preventing crimes are being completed.

The success of the investigation of any crime is largely determined by the ability to penetrate not only the criminal law, but also the criminalistics nature of it. The basis of the same investigation methodology is the disclosure of the content of this entity, as well as an analysis of the activities of the relevant bodies to identify, uncover and investigate the crime.[21]

Correctly to understand the criminal nature of the deed is possible only under certain conditions. To do this, it is necessary to have an idea of the typical criminologically significant features of various types of criminal activity, as well as to be able to purposefully detect the necessary forensic information in each specific crime and draw a parallel with the forensic characteristics of the relevant type of crime.[22] Forensic methodology on the basis of scientific study and generalization of all types of forensic information facilitates the creation of the most sophisticated methods of disclosure and investigation of crimes and the development of relevant practical recommendations on the use of criminalistics techniques and tactics specific to this type of crime.

The result of scientific generalization of information about a certain group (type) of crimes is the criminalistics characterization of the crime, which is one of the most important structural elements

[21] Internet Corporation for Assigned Names and Numbers // Materials of the Internet Registrar's Site, available at: https://www.icann.org/resources/pages/registrars-0d-2012-02-25-en

[22] Fischer, M., An Investigation of Fraud in Nonprofit Organizations: Occurrences and Deterrents. - Nonprofit and Voluntary Sector Quarterly, 2007, Vol. 36, No. 4, 676-694

of the investigation methodology. Forensic characteristics serve as a key, starting point for the presentation of methodological recommendations.

At the heart of the criminalistic characterization of the crime lie the data of the study of the material and ideal traces left by them as a result of the interaction of the subject of the crime with other persons, material and other objects of the environment, which point to the forensic signs of the crime, the criminal, various circumstances, this action, possibly not essential for his qualification, but important for the disclosure of the crime.[23] The basis for constructing an information model of a certain type or group of crimes is the data of analysis and generalization of materials of judicial and investigative practice and forensic research.

In this process, the formation of elements that make up the structure of this characteristic, proceeding from the object of study, cannot fail to take into account the general structure of criminal activity and is characteristic of its corresponding type.

At the same time, this structure cannot but be coordinated to a certain extent with the criminal law, criminal procedural and criminological directions of searching for relevant information about the crime.

Forensic characteristics, based on an analysis of its content, in our opinion, should include:

1. Object of infringement.

2. Characterization of the initial information.

3. The system of data on the method of crime:

   3.1 Ways of preparation;

   3.2 Ways of committing;

   3.3 Ways of concealing a crime.

4. The circumstances of the commission of the crime (place, time and circumstances of the commission of the crime).

[23] Kranacher M.J., Forensic Accounting and Fraud Examination, John Wiley & Sons Ltd, Chishester, 2012

5. Data on the identity of the perpetrator and the likely motives for the crime.

6. Data on the identity of the victim.

7. Consequences in the form of any changes caused by the crime, which are expressed in such components:

a) characteristic traces, their localization and interrelation caused by official and off-duty actions and connections, way of life (evidence of behavior);

b) material and physical damage, moral damage, damage to business reputation, caused by a crime.[24]

These elements are fully included in the forensic characteristics of Internet fraud.

Analysis of modern forensic literature and practice allows us to conclude that the forensic characteristics of Internet fraud have not been disclosed to date. This is explained by the specifics of the commission of the crime, since the anonymity afforded to its users by the Internet, the possibility of reaching a large audience, the high speed and the much lower cost of disseminating information compared to traditional means makes the Internet the most convenient tool for fraudulent activities.[25]

It is necessary to emphasize that all these elements of the criminalistics characteristics of Internet fraud are interrelated and form a unified system. The revealed information about one of them allows us to make probabilistic conclusions about an unknown or insufficiently known other element (circumstance) of the crime under investigation.

Based on the foregoing, we can conclude that the criminalistics characteristics of Internet fraud allows the investigator to make substantiated versions of all the circumstances of the crime committed, including. on the location of the swindler, and also to carry out a quick search for the fraudster, to ensure the completeness, comprehensiveness and speed of the investigation, to determine the nature of the tracks and their location, to identify means and methods for their detection and consolidation, as well as measures to prevent fraud.

[24] Chen H., Intelligence and Security Informatics. First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, June 2-3, 2003, Proceedings. 1st ed. Springer, Berlin 2003, p 232-248.

[25] Chua (2004). *Supra nota*. P. 37.

According to some experts, one of the most accurate indicators of the state of cybercrime is the level of spam. In October 2006, his level went over 90% of all mail traffic (Postini statistics). Only in the last two months of 2006 the volume of spam increased by 60%, and the attackers successfully mastered the new technology of graphic spam with content variations.[26]

The volume of spam is a good indicator of the level of cybercrime, because garbage letters are usually sent out with the help of botnets, that is, networks of computers «zombies» - home computers that are infected with a virus and send spam on a command from the «owner» of the network. In a criminal environment, botnets are considered a very liquid commodity and are constantly sold and bought. The more home computers are infected, the higher the level of spam on the Internet.

To date, according to experts, spam botnets contain about 3-4 million PCs. The content of the botnet is an extremely profitable business, which is the main source of income for modern cybercrime groups. For example, Israeli botanist Gadi Evron estimated the yield of botnets in 2016 at $ 3.6 billion.[27] This money was obtained mainly from phishing, by luring people to fake websites through spam.

According to the report of Symantec corporation compiled for the period from January to June 2017, 58429 active bot-node was found, which is 14% less than half a year earlier. At the same time, 29% of such botnets are located on the territory of China (but at the same time most of the managers of these botnets - is located in the United States)[28].

Another proof of the heyday of cybercrime in 2016 is the change in the time of hacker attacks. It used to be nights and days off. Now the attacks are going on during the day on weekdays. In other words, cybercrime has become a routine job for many people, except that this entry is not included in the workbook.

According to the report of Aladdin Knowledge Systems, the level of activity of threats contained in web content for 2016 increased by 1300%. In total for 2016 there were 104082 attacks (for comparison, in 2015 there were 825730). The above data indicate that spyware and Trojans

[26] Gregg, Dawn G., The Role of Reputation Systems in Reducing OnLine Auction Fraud. International Journal of Electronic Commerce 10(3), April 2006, p 95-120.

[27] See more at https://www.crunchbase.com/person/gadi-evron/timeline/timeline

[28] Symantec report (2017)

penetrating users' computers from the Global Network are leading the first positions in the report on the most dangerous threats.[29] [30]

Further development of the theoretical foundations of the criminalistic characteristics of Internet fraud is an actual scientific task, conditioned by the needs of the criminalistic theory and the practice of identifying and investigating crimes of this type.

2.2. The subject, situation and method of committing a crime

Deception with Internet fraud is different from any other fraud not only in that it is used to acquire property. Here, the character of the object of encroachment and, accordingly, the purpose that the offender sets, determines the content of deception and often its form.

From the above definition, it is seen that deception can occur both in active and passive forms. Thus, an active form of deception would be advisable if as a deliberate misrepresentation of the truth contained in the alleged victim information, but passive as a silence about the true facts. As for the Internet - fraud, it usually takes place in an active form: by sending out spam or fishers letters, direct work of scammers in chat rooms, etc.

Thus, it would be advisable to characterize the active form of deception as a deliberate distortion of the truth contained in the victim's information, but there is also a passive form of deception, which should be characterized as silence about the truth.

The content of fraudulent deception is the circumstances in respect of which the fraudster misleads the victims. These circumstances are very diverse. Deception can concern objects, persons, actions, their actual or legal properties. Events that are misleading can be related to present, past or future

[29] See the whole Alladin Knowledge Systems 2016 report at https://www.surf.nl/en/knowledge-base/2016/cyber-threat-assessment-2016.html

[30] See the new Alladin Knowledge Systems 2017 report at https://www.surf.nl/en/knowledge-base/2017/cyber-threat-assessment-2017.html

Some circumstances in respect of which the criminal lies lie directly serve an imaginary reason for the transfer of property. Other circumstances, not being grounds for the transfer of funds, are used by the criminal in order to create the prerequisites for another fraud or to inspire confidence in himself, and then with great ease to deceive or abuse the trust of the victim. They are also included in the content of fraudulent fraud, tk. the victim takes into account these circumstances when he decides on the transfer of property.

In the legal literature, it is generally accepted that fraudulent deception can be committed in any form: verbally, in writing, through various actions and by inaction. Internet fraud is characterized by a written form laid out on various Internet sites.

Thus, forensic classification of Internet crime by means of committing and criminal purposes of a crime, includes the following list of fraud actions:

1) Illegal connection to the information and telecommunication network Internet:

- illegal receipt and use of other people's credentials for access to the network

Internet (logins and passwords);

- partial substitution of own account data by strangers (MAC and IP-addresses) with the purpose of

- unauthorized access to the Internet;

- unauthorized connection to the telecommunication operator's network in order to avoid payment for received Internet services.

2) Creation, use and distribution of network malicious programs for COMPUTER.

3) Illegal production, storage, distribution, advertising and (or) public demonstration of information prohibited for free circulation, committed using the Internet:

- illegal production, storage, distribution, advertising and (or) public demonstration of pornographic materials committed using the internet;

- illegal receipt and disclosure of information constituting commercial, tax or banking secrets committed with the use of the Internet;

- violation of the secrecy of correspondence, telephone conversations, postal or other messages transmitted over the Internet;

- illegal collection or dissemination of information about the private life of a person constituting his personal or family secret, including personal data, committed using the Internet;

- an insult inflicted by spreading defamatory information in the information resources of the Internet;

- the incitement of hatred or enmity, as well as the humiliation of human dignity, committed using the Internet.

4) Violation of copyright and related rights, as well as illegal use of another's trademark, committed using the Internet.

5) Fraud in the provision of Internet services.

Some circumstances in respect of which the criminal lies lie directly serve an imaginary reason for the transfer of property. Other circumstances, not being grounds for the transfer of funds, are used by the offender in order to create a premise for another deceit or cause confidence in yourself, and then easily deceive or abuse the trust of the victim. They are also included in the fraudulent content. The victim takes into account these circumstances.[31]

Some circumstances in respect of which the criminal lies directly serve an imaginary reason for the transfer of property. Other circumstances, not being grounds for transfer is also a passive form of deception, which should be characterized as silence about the truth.

Thus, the criminal law provides in the most general form an indication of two main ways of illegal possession of property: deception and abuse of trust. It is noted that a person in charge of or under the protection of which the property was or its owner, the owner, himself transfers such property to the guilty (or the right to it), believing that the latter has the right to this property or performs certain actions promised to the perpetrator for the victim. At the same time, the victim has an erroneous opinion about the profitability or mandatory transfer, or assignment of the right to

[28] Комаров А.А, Криминологические аспекты мошенничества в глобальной сети Интернет, Саратовская государственная академия права, Кандидатская диссертация, Саратов, 2011

property to the guilty, being misled. Voluntary transfer to the victim of property is a mandatory sign of fraud, although this voluntariness is actually fictitious, as the actions of the owner of the property are in fact due to misleading or unjustifiable trust.[32]

The legislator himself does not define the concept of deception and abuse of trust. Deception as a way of fraudulent acquisition of another's property consists in communicating to the victim false information or in concealing certain links, the significance of which would be essential for his subsequent behavior.

Deception with Internet fraud is different from any other fraud not only because it is used to acquire property. Here, the nature of the object of encroachment and, accordingly, the purpose that the offender sets, determines the content of deception and often its form.

From the above definition, it is seen that deception can occur both in active and passive forms. Thus, it would be advisable to characterize the active form of deception as a deliberate distortion of the truth contained in the victim's information, but passive as a silence about the true facts. As for Internet fraud, it usually takes place in an active form: by sending out spam or phisher letters, direct work of scammers in chat rooms, etc.[33]

Thus, it would be advisable to characterize the active form of deception as a deliberate distortion of the truth contained in the victim's information, but passive as a silence about the true facts.

For example, by abusing the trust of a construction company, the fraudster on its behalf starts on the Internet to offer to build apartments under construction, using the present title documents of the company.

Acting in a fraudulent manner on behalf of this company, the fraudster enters into valid investment contracts for future flats, receives cash on these contracts, but does not perform any work under these contracts, disappears with cash, which causes significant damage to the victims.

There is also a passive form of deception, which should be characterized as a silence about the truth.

[32] Burns Ronald G., Assessing law enforcement preparedness to address Internet fraud. Journal of Criminal Justice, Elsevier, vol. 32(5), 2004, p 477-493.

[33] Chua (2004) *Supra nota* P. 25.

The content of fraudulent deception is the circumstances in respect of which the fraudster misleads the victims. These circumstances are very diverse. Deception can concern objects, persons, actions, their actual or legal properties. Events about which an error is created can relate to the present, past or future time.[34]

Some circumstances in respect of which the criminal lies, directly serve as an imaginary reason for the transfer of property. Other circumstances, not being grounds for the transfer of funds, are used by the criminal to create the prerequisites for another fraud or to inspire confidence in himself, and then with great ease to deceive or abuse the trust of the victim.[35] They are also included in the content of fraudulent fraud. the victim takes into account these circumstances when he decides on the transfer of property.

For example, on the Internet, it is often suggested to buy various access codes for downloading movies, music files, pictures, etc. In this case, it is suggested to send an SMS message to a certain number. Signs also from which country to which number to send this message.

After sending an SMS message, it often answers that the access code will be sent to the client after receiving a payment confirmation, but after that no access codes come in, and money is written off from the customer.

In this case, the reason for sending money is a false message of intention on the part of the client to purchase an access code (ie, fraud in intent).

In the legal literature, the common opinion is that fraudulent deception can be committed in any form: verbally, in writing, through various actions and through inaction.

Internet fraud is characterized by a written form laid out on various Internet sites.

Abuse of confidence is most often combined with deception. Usually the criminal tries, first of all, to win the trust of the victim, so that it is easier to commit deception.

[34] Комаров (2011) *supra*
[35] Chiemeke (2006) *supra*

Deception in many cases could not have been done had the victim not had some confidence in the deceiver. Abuse of trust is misleading about the true intentions and goals of the perpetrator, combined with the unfair use of trusting relationships with the victim.[36]

In particular, scammers often use various websites, similar to the sites of well-known brands, for various purposes to abuse trust, different names that are associated with Internet users with a quality mark.

At the same time, fraudulent abuse of trust should not be identified with other crimes provided for in special cases. In the commission of fraud, the abuse of trust is a necessary element of the illegal circulation of property in its favor or the benefit of others.[37]

To summarize previous - currently, the following are the main types of fraud on the Internet:

- phishing;
- fraud with payment plastic cards;
- Internet fraud in the securities market;
- schemes of auctions and retail trade on-line;
- business opportunities / «home-work»;
- Internet fraud in the mobile cellular market;
- cybernition, etc.[38]

According to the definition of Dr. Web, phishing is an Internet fraud technology that involves the theft of personal sensitive data, such as access passwords, bank and ID card data, and so on. With the help of spam mailings or email worms, potential victims are sent false letters allegedly on behalf of legal organizations, in which they are asked to go to the forged site of the institution and to confirm passwords, PIN codes and other personal information used by attackers to steal money from the victim's account and in other crimes.

[36] Fischer (2007) *supra*
[37] Комаров (2011) *supra*
[38] Staples, H., The legal status of third country nationals resident in the European Union / Staples Helen II European monographs. Kluwer Law International. 2008, p 290.

According to the report of the association APWG (Anti-Phishing Working Group)[39], in April 2016 there was a sharp increase in the number of unique phishing sites.

According to the APWG report, if in March 22,836 fraudulent sites were recorded, in April their number was 58,290[40]. MarkMonitor specialists note such a rapid increase in that phishers began to place a lot of URLs on the same domain.[41] This tactic was first discovered in October last year.

In April 2016, the number of brands that were becoming subject to forgery also increased. If in March scammers actively exploited 166 brands, in April their number increased to 174, and the increase did not go due to traditional for phishers financial institutions, but due to VOIP-services and social networks. At the same time, the most «popular» among scammers are still the sites of financial companies, they account for 92.5 sites-deceptive.[42]

In May 2016, according to the APWG report, the number of unique phishing emails and phishing of websites decreased slightly compared to April 2016. So, if in April 2016 55643 phishing websites were detected, in May they were fixed at 18,000 less (37438). At the same time, the quality of such sites is noted.[43] Researchers at MarkMonitor explain this growth with the relatively new tactic of phishers - placing on the same domain many Fisher URLs, the number of which reaches several thousand. All this is done to «deceive» the protection tools built into Microsoft Edge and FireFox browsers.

In addition, databases of phishing addresses are constantly growing. And it's not just that the number of phishing sites is increasing. This is also related to the migration of phishing sites: they are constantly moving from one server to another. The average life span of a phishing site is less than 4 days, after which the site is moved to a new site, so the growth of the database address database is quite large. So, if the average length of the URL of the phishing page is 70 characters, and an average of 1500 new addresses are added to the open phishing-address databases every day, the database will increase by almost 95 Mb per year, if the tempo of adding new phishing addresses is maintained.

[39] See more at https://ecrimeresearch.org/
[40] See APWG Phishing Attack trend Report Q1 and Q2 2016 and others at https://www.antiphishing.org/resources/apwg-reports/
[41] MarkMonitor report available after registration at https://info.markmonitor.com/online-barometer-fraud
[42] APWG Phishing Attack trend Report Q1 and Q2 2016
[43] *Ibid*

According to the Radicati Group report, the number of phishing attacks is constantly increasing. The forecast for 2018 is 404 attacks per day.[44] The risk of this kind of attack for companies is obvious, since the theft of data in certain sectors can seriously affect the operation of the company.[45]

Increasingly, this type of crime, such as fraud with payment plastic cards, gets. Fraud with payment plastic cards, as a serious problem, arose in the 90s of the 20th century and over the past 10 years the annual losses have increased more than 20 times and represent tens of billions of dollars.[46]

With the development of the personal computer market and the increase in the volume of the Internet audience, the volume of electronic banking also increases accordingly. For example, in Germany, from the beginning of 2017, the system of remote banking services or e-banking is offered by almost all the major banks of the country, with many banks offering free banking services to their ordinary customers along with a «salary» card. This allows banks to save on office space and operators. Estonia's biggest banks like Swedbank, SEB, etc have overcome to purely internet-based banking in 2011, when additional fees were brought in for all physical client services. For customers, this is also more profitable (operations through the Internet are cheaper) and more convenient.

In European countries, according to a recent poll conducted by Symantec, consumers place online banking services first among all activities on the Internet that make life easier for them. Thus, 86% of respondents believe that banking online services save them at least 5 hours a week, and more than one in five (21%) considers it possible to do without personal visits to the bank due to online banking services. The survey also showed that when consumers need advice or assistance in protecting personal information, they first turn to their financial institutions (54%), and then to security companies such as Symantec (29%)[47].

The number of people who use online banking services is growing all over the world - they pay bills, manage their bank savings, calculate the most favorable loan terms for themselves. In the analytical company eMarketer believe that only in the US, about 80 million adult Internet users

[44] See more at https://www.radicati.com/?page_id=54
[45] Hecker B., Europaisches Strafrecht. Springer-Verlag Berlin Heidelberg. 2005. p 94.
[46] U.S. consumers and cyber crime – Statistics & Facts 2017
[47] Symantec report

this year will perform some kind of banking operations on the Net. This is 9.5% more than in 2016 - such information is contained in the report «The Banking and Bill Paying Online report. »[48]

Forgery of credit cards, computer theft took the nature of a real disaster in the US, Italy and other countries. Companies, especially banks, seek to hide the facts of computer theft, because they fear the fall of the confidence of investors, shareholders or partners. Therefore, in official statistics, the scale of losses is almost not recorded. And the victims often do not suspect that they were robbed. Experts believe that in the United States with the help of computers from banks abducted four more than with armed robberies.[49]

According to the international association APACS (Association for Payment Clearing Services) in the first half of 2017 there was a sharp increase in the activity of online scammers in the field of online banking operations.[50]

The main focus fraudsters made on the users of online banking services. The number of officially registered fraud cases for the six months was 5 059, which is 16% more than in the last 6 months. 2016 year. The amount stolen by fraudsters for 6 months. 2017 exceeded 84 million dollars. In total, in the first half of 2017 scammers stole about 420 million dollars from plastic cards, which is 9% less than in the last 6 months of 2016.[51]

Also, experts note an increase in cases of forgery of bank cards. In the first half of 2017, about $ 93 million was cashed over counterfeit cards, which is 16% more than in the previous six months.

In the UK, the number of counterfeits with bank cards is also growing steadily reports. Only two-thirds of private owners of bank accounts feel protected from fraud. This conclusion was made by experts of the computer company «En-Crop» based on the results of the public opinion poll. According to official figures, every year in the United Kingdom, scammers inflict a loss of £ 1m to owners of «credit cards». Fictitious transactions involving the use of foreign confidential data occur every eight seconds. 27% of Englishmen think that their banks cannot cope with the task of increasing the security of contributions and payment means of their clients. 62% of respondents

[48] Electronic Crime Scene Investigation: A Guide for First Responders. US department of Justice, 2nd editon. 2008.
[49] 2016 Financial Cybersecurity Report, (2016). SecurityScorecard.
[50] An integrated vision to manage cyber risk, 2017, EY
[51] *Ibid*

stated their intention to immediately abandon the services of a financial institution - if they consider that it is inferior in the fight against scammers.

According to the British newspaper The Guardian, the damage from Internet fraud in the UK banking sector alone grew by 15 percent in 2017 compared to 2016.[52] The police also state that official statistics do not reflect real damage. According to police estimates, Internet fraud costs the UK economy more than $ 3 billion a year.[53] Banks do not report attacks on their systems, possibly not wanting to make these cases public, or believing that law enforcement agencies are not able to cope with this problem.

It should be noted that the most Internet-criminalized regions of the world include highly developed countries (primarily the USA, Great Britain, Canada, Australia), developing countries (including Russia, Romania or, for example, Indonesia), and even entire African regions, which we are used to consider backward (from Nigeria to Togo).[54] Forms and methods of computer theft, the most common in different countries, naturally differ from each other and depend on what types of web services are most often used by their citizens: here and the already mentioned «air trade», and the use of fake or stolen credit cards, and scams with bank accounts and transfers, and much, much more.[55]

According to a report from Symantec, compiled for the period from January to June 2017, 61% of all DoS-attacks were committed to web-resources located in the United States, and 25% of all network attacks occurred from the territory of the United States, which ranked first in this indicator in the world.[56]

Along with fraudulent activities that result in direct damage, "less harmful" identity theft is evolving actively. For example, in Estonia, for the years 2010-2014, due to cases involving the illegal use of another person's identity, a total of 383 criminal records were reported, in 2015, 146 criminal records and 146 criminal records in 2016[57] mis näitab, et nimetatud kuritegude registreerimiste arv on kasvavas trendis. As Merika Nimmo pointed out in her article that although

[52] The Guardian, (2017). UK fraud hits record £1.1bn as cybercrime soars,
[53] See more at: https://www.actionfraud.police.uk/news
[54] Grazioli (2010). *Supra*
[55] Longe Olumide. On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. The African Journal of Information Systems, 2011, Vol 3, Issue 1.
[56] Symantec report (2017)
[57] Registreeritud kuriteod 2012–2016. Baromeeter. Justiits-ministeeriumi kriminaalpoliitika osakonna võrgukodu. Available at: http://www.kriminaalpoliitika.ee/et/statistika-ja-uuringud/baromeeter

identity theft is increasingly being reported, many criminal cases remain open without reason on the grounds that there is no basis for criminal prosecution.[58] Erkki Hirsnik[59] conversely claims, that the overall numbers of registered criminal cases is way lower, but he also affirms that the number of internet fraud actions is in rising trend.

To summarize the data pointed out in current chapter, it is clear, that internet fraud is in rising trend both in Estonia and worldwide. The affirmed fact of the rising trend of internet fraud proves authors hypothesis, that the methods of fighting internet fraud used today are ineffective and need to be changed or improved.

2.3. General characteristics of perpetrator

Recently, a large number of studies and publications have appeared, affecting various aspects of computer crime. Almost in each of these works, the authors attempted to classify computer criminals, singling out homogeneous groups among them. As one of the basic classifying traits in investigating forensic aspects of the KP, many authors consider the goals and scope (kind) of illegal activity. However, in our opinion, the number of homogeneous groups isolated and studied for this trait is inadequate and lags behind the modern realities.

First of all, it should be noted that among specialists there is still no single interpretation of the term «hacker». Initially, a hacker was a highly professional programmer who could develop and modernize computer programs without having detailed specifications and documentation for them. This interpretation was prevalent at the turn of 70 ... 80th years of the last century, when the world hacker movement was born and developed.

Later, with the growth of the scale of Internet fraud and turning it into an independent kind of crime, the term acquired a criminal connotation and began to mean a computer cracker who could illegally gain access to a computer network.

[58] Nimmo (2017). *Supra*.

[59] Hirskin, E. Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid, Juridica, 2014/8, P. 611-624.

However, most authors reasonably believe that the use of the term «hacker» is more preferable for the latter category of illegal subjects.

The main difference between these categories is, in authors opinion, not in age or skill level (novice, professional, super-professional), but in the nature of the impact on information and in the target setting. The subjects of both categories are looking for and analyzing vulnerabilities in IP hardware and software and are hacking computer systems and networks (CSN).

Hackers, for example, often have research objectives, do not have harmful effects on information and report the results of their attacks. On the contrary, the crackers carry out hacking CSN to obtain unauthorized access to other information, the nature of the impact on which is much more dangerous, depending on their motives.[60]

When Internet fraud is committed most often we can talk about the following category of Internet criminals

- carders - specialize in fraud with plastic cards, paying their expenses from other credit cards. A typical carding procedure is to copy the information contained on the magnetic strip of the credit card (dump) and produce a fake phantom card with a copied dump on it or to obtain an individual Pin code from the owner of the real card, for example, using social engineering techniques.

- cybercrooks - specialize in unauthorized entry into the KSS of financial and banking institutions and closed KSS of state power structures and bodies. Use KCC for theft of money, obtaining valuable financial information. A popular commodity is credit information, information databases of law enforcement agencies and other government and commercial structures.[61]

- phishers, whose purpose is to take advantage of fraudulent personal data from customers of online auctions, online stores, money transfer services and other confidential information. Constantly improved by scammers, various «tricks» are directed, in the main, to those who are too gullible or inattentive, who themselves (voluntarily) part with confidential information when they

[60] Casey E., Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edition. 2014. P 475, 750, 752, 38, 175

[61] For example: USA vs Nikolay Nasenkov and Aleksandr Kalinin casus, in which according accusasation Kalinin and Nasenkov by hacking insider information of finantial institutions which they used to gain profit.

are asked to repeat the password entry, to provide the account number and password for registration of the purchase or money order, register on the false website of the Internet store, etc.[62]

- Spammers are engaged in mass (more than 5 addressees) sending unsolicited (often anonymous) ads using electronic communications, primarily by e-mail.

- pornographers - use the WWW's capabilities for paid distribution of pornographic materials. More than 75 percent of all child pornography is distributed on the Internet, where, according to some estimates, there are almost 40,000 pornographic sites.

- cybersquatters - seizure of domain names for profit. Domain names are often called «real estate» of the online age. A well-chosen name can by itself provide a sufficiently strong flow of visitors, and hence potential customers: a good name is intuitively located and easily remembered. Awareness of the value of domains is constantly growing, and their price is also growing.

- phreakers specialize in the use of telephone systems, hacking of digital telephone exchanges of telephone companies, unauthorized receipt of codes for access to paid ISDN services, theft and forgery of telephone cards, etc., in order to avoid payment for services rendered in ITT sphere.[63]

The «portrait» of the average Internet rogue has already been drawn up: this is about a 35-year-old man who trades fraud using his personal computer at home and during his free time. He steals, as a rule, little by little: 32 successful «raid» of 100 bring him less than $ 500, and only in three cases he manages to pocket over 10 thousand. Moreover, according to law enforcement agencies, these three cases are usually the fastest and are being investigated.[64]

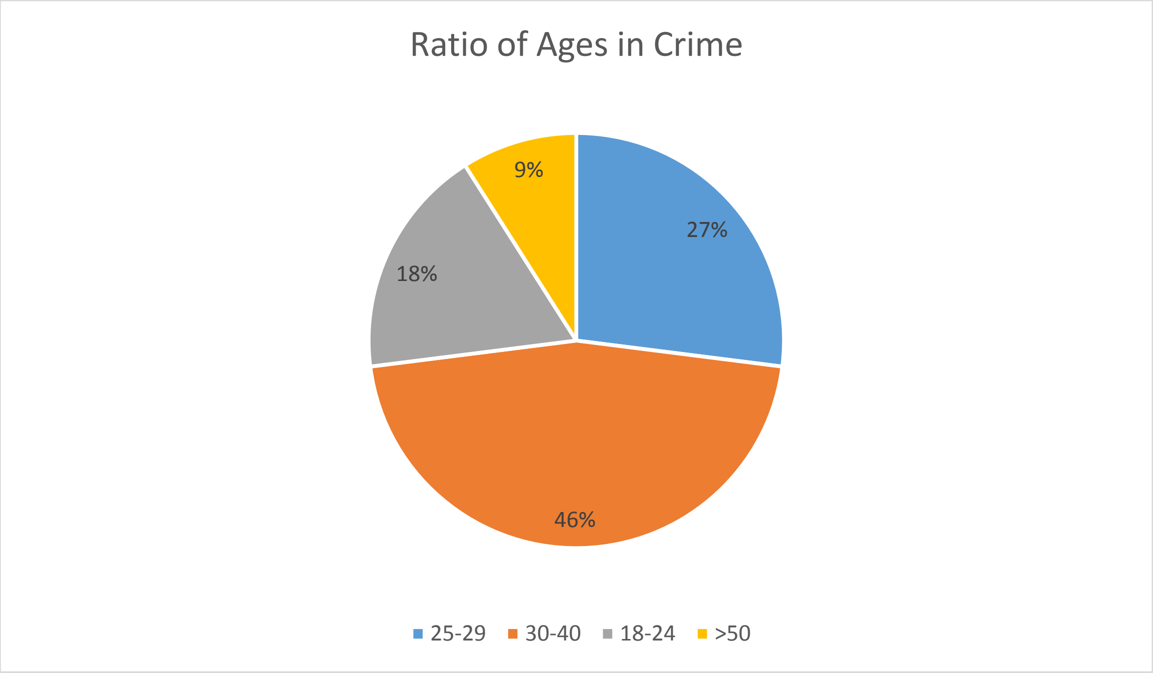
It is important to mention that the anonymity and disguise technologies used on the internet allows the criminal to overcome psychological barriers that prevent him from committing a crime outside cyberspace. The anonymity factor of the global network also gives the cyber criminals the opportunity to communicate with their accomplices without attracting attention. Which makes a

[62] Very common are phishers attacks who fake well known and respectable brands. For example Apple. See more at: https://support.apple.com/en-us/HT204759

[60] Jaishankar, K., Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC press. 2011. p 74

[64] *Ibid*

cyber-criminal different from “real world criminals” with different behavior template mostly smart, well informed and prepared to face the consequence.[65]


Ratio of Ages in Crime

Knowledge of the identity of the perpetrator is necessary. They allow to formulate concepts of crime prevention. Crime prevention is a multi-level system of targeted state and public measures to identify, eliminate, reduce and neutralize the causes and conditions of crime, certain types of crimes and specific crimes, as well as to prevent people from returning or returning to a criminal path whose living conditions and behavior indicate such an opportunity.[66] Measures on prevention of internet fraud will be discussed in the fourth chapter of current paper.

[65] Тарасенко, В., Киберпреступность: Международный уровень решения проблемы. *Электронный сборник статей по материалам XII студенческой международной заочной научно-практической конференции*, Новосибирск, 2017, p 418-423

[66] Jaishankar (2011). *Supra nota*. P. 28

2.4. General characteristics of the circle of victims

Victims of fraud can be divided into two main groups, based on they are classified based on the activity of their behavior after receiving information about how that they were victims of scammers:

1. Victims who are interested in the successful investigation of a crime, provide the law enforcement bodies with all the information known to them and actively promote them in other forms.

2. Victims with passive behavior. Representatives of this group, as a rule, are limited to filing an application and do not follow the progress of the investigation, or do not take any action at all to attract fraudsters to criminal liability.

There is also another group of victims, whose representatives are inclined hide their status, and even, in some cases, oppose law enforcement agencies in conducting investigations. It can be both physical and legal persons. The reasons for such, at first glance, illogical behavior is different and lie, most often, in fear: fear for business reputation, fear of disclosing certain aspects personal life, etc.

It seems that this group can act as one of the criteria for determining the level of latency of a crime. Computer crimes in general and Internet fraud, in particular, initially have a fairly high level of latency. To solve this problem, we propose to work on improving confidence in law enforcement. This will not only increase the number of violations, but also to attract more victims to investigation, and also to operate with more complete information and, therefore, more honestly investigate Internet fraud. Carrying out such work is especially an actual for the prevention of crimes, the peak of which falls on the best time of the year. In such cases, awareness-raising activities will on the current criminal situation and keep in touch with the most serious threats at the moment.

Fate of fraud on the Internet can be every fourth. The report was compiled on the basis of a survey of the owners of 2 thousand households with access to the Internet, conducted by the Consumer Reports National Research Center. Over the last six months of 2016, 34% of respondents have encountered spyware on their home computers, 38% - with viruses, and 8% of respondents at least once in two years came across the «bait» of phishers, reporting their details on fictitious sites. Each such incident, ultimately, resulted in a loss of an average of $ 200. 17% of users do not have antivirus software.[67]

Experts have already collected rich statistics showing that from web-theft business structures suffer much more than private individuals. Men are victims of such crimes more often than women, and older people are more likely than young people.[68]

According to a report from Symantec corporation compiled for the period from January to June 2017, about 95% of network attacks were aimed at simple home users of the computer. Of the ten newest and most serious families of malicious code, four were Trojans, three were pure viruses, one was a network worm and two were network worms with a virus component. Also over the reported six months, more than 212 thousand unique malicious code instances were registered, which is 185% more than a year earlier, and 46% of virus files were transmitted via the SMTP protocol, which was the most popular way to deliver malicious code[69]

Thus, Internet fraud is a socially dangerous guilty act committed on the Internet and aimed at capturing the property or money of Internet users by deception or abuse of trust. Investigation of it can have two approaches: 1) when the investigator starts with planning investigation through the information provided by victim, or so to say "victimologic[70] approach"; or 2) approaching to the investigation through technology used by the perpetrator, or in another words "technologic approach". Victimologic approach is important to define the circle of potential victims, and foresee legal measures to defend them, which means that through victimologic approach fraud prevention is made. Methods of investigation and evidence gathering are evaluated in the third chapter of current paper.

[67] Olmstead Kenneth, Americans and Cybersecurity, Pew Research Center, 2017

[68] Sean Xu, Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China, Journal of Electronic Markets, Vol 14, Issue 1, 2004, p 13-24.

[69] Symantec report 2017

[70] Victimological research involves studying both the total contingent of victims of crimes and victims of certain types of crimes. The study of the specifics of victimization of victims of specific crimes allows for a more differentiated approach to the issues of victimological prevention and, thus, to provide a general preventive effect. See more about forensic victimology: Turvey Brent E., Forensic Victimology, Academic Press, Elsevier Inc, 2014, p 517-558

CHAPTER 3. THE ISSUES OF ORGANIZING AND SECURING THE INVESTIGATION OF INTERNET FRAUD

3.1. The initial stage of the investigation of Internet fraud

Investigation of fraud, which was committed using computer technology, is conducted on the basis of planning, the basis for which is the initiation of a criminal case on the basis of available documents.

An integral part of the initial stage of the investigation of Internet fraud is the planning, nomination and review of versions that play a crucial role in building an investigation plan. Versioning and testing are the basis for building a plan. Among the most developed problems of criminology is the doctrine of the forensic version.[71]

The investigator's versions are investigative versions. They can be brought forward by another person who is involved in the investigation. Such versions are one of the types of forensic versions. In the investigative versions all the most important regularities inherent in this forensic category are manifested. Therefore, considering the problem as a whole, you can pay special attention only to investigative versions.[72] Forensic version is a generic concept, it refers to a higher level. Investigative, expert, judicial, operatively-search versions are conceptions specific. When investigating Internet fraud, the investigator must take into account the wide variety of facts that form the basis of the version that can be put forward.[73]

At the stage of acquaintance with the information provided, the investigator can conduct an analysis of the materials that he has. He can trace the connection between individual episodes of

[71] Атаманов, Руслан Сергеевич, Основы методики расследования мошенничества в сети Интернет Московская государственная юридическая академия, Кандидатская диссертация. Москва, 2012

[72] Wright Ryan T., The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. Journal of Management Information Systems, Volume 27, 2010 - Issue 1, 2010, P. 273-303.

[73] Атаманов (2012). *Supra*.

the crime. Thus, he reveals the motive of the crime. It is the motive that forms the guilty line of behavior.[74] Comparing the tracks that were discovered during the investigation and taking into account the specifics of Internet fraud, in order to formulate the version, the experience of professionals is used. He plays a huge role in explaining certain facts, information about which is missing.

Having received primary information about fraud, using Internet technologies, the investigator makes general versions. Primary information can be a statement, an inspection of the scene of the incident, a survey of the victim or eyewitnesses. These versions are typical in the following cases:

- when fraud committed using Internet technologies was indicated to the victims;
- in the circumstances listed by the victim there is a composition of another crime;
- The victim submits an application for fraud with the help of Internet technologies, but information has been received about the possible staging of criminal actions.

In most cases, the materials that were provided for the initiation of a criminal case may contain data that are sufficient to advance versions. Certain investigative actions are recommended by experts in criminalistics as the most effective in order to collect evidence.[75]

Inspection of the scene plays a huge role in the investigation of Internet fraud, but the role of this inspection is sometimes underestimated, the situation is fixed, which is perceived visually by the investigator. And not in all cases they resort to the help of technical and criminalistics means. Schemes and plans are not drawn up. The inspection protocols do not reflect the nature of the criminal's influence. The testimony obtained during the interrogation is not detailed. This has a negative impact on the possibility of nominating different versions of the theft, in which computer technology is used.[76]

If there is evidence of the perpetrator, the victim and the witnesses, then the versions of possible motives and the purposes of the theft may be the initial stage of the investigation. For the most expedient and purposeful organization of the investigation, it is necessary to plan the investigation

[74] Chen (2003). *Supra nota* 209-223

[75] А.А. Комаров, Криминологические аспекты мошенничества в глобальной сети Интернет, Саратовская государственная академия права, Кандидатская диссертация, Саратов, 2011

[76] Sean Xu (2004). *Supra*.

of Internet fraud. This increases the level of objectivity, allows you to quickly, fully and comprehensively establish the circumstances of the crime and begin to search for and expose the offender.

In drawing up a work plan for the criminal case, the investigator must consider all future actions, select methods and means by which he can ensure a productive collection and evaluation of evidence in the current case. In the literature on forensic science, you can find a variety of definitions of planning investigations. What is common is only an approach to the very design of the investigation plan, as to the process of the mental. Planning is one of the indispensable conditions for investigating Internet fraud. It is a thought process, which consists in identifying the tasks of the investigation, determining the ways to solve them and ways in accordance with the requirements that the law makes.[77]

The basis for planning is the actual basis. This basis is formed by information about the thefts, which are made with the use of technologies related to the Internet, containing the signs of committing a criminal act. The ways of obtaining this information are procedural, as well as operational-search. Information obtained by operational search means cannot be evidence in this criminal case. It is necessary for the investigator to plan and solve tactical tasks. The definition of investigation tasks, versioning, path selection and verification methods depend on how complete the actual data are.

At the initial stage of the investigation, the information obtained about the crime or the event containing its signs is limited. It is difficult to draw up an investigation plan. This obliges the investigator to review and supplement the work plan as new facts are established. Planning is a continuous process. Termination of it may be due to the termination of the investigation. An objective prerequisite for planning is the investigator's availability of factual data about the crime committed. The level of his theoretical knowledge and his professional experience are the basis for making the right decisions related to the conditions of consideration.

Shortly investigative work has a number of shortcomings[78]:

[77] Smith Russell G., Urbas Gregor, Controlling Fraud on the Internet: A CAPA Perspective. Australian Institute of Criminology. Research and Public Policy Series, No. 39. 2001

[78] Herlin-Karnell, E. White-Collar Crime and European Financial Crises: Getting Tough on EU Market Abuse. – European Law Review, No.2012/4, 2012, p 481–494

- low detection of dangerous crimes;

- Investigations are conducted incompletely, often the most important facts of the case are not clarified;

- Investigations are often protracted, which is the reason for incomplete disclosure of committed criminal acts and the reduction of criminal penalties.[79]

In this thesis, we will consider in detail the above-mentioned shortcomings in the conduct of investigative work and their causes.

Correcting the current situation is possible through the effective planning of Internet fraud investigations. Main reasons:

- The official commitment that is necessary to effectively and comprehensively address the challenges associated with investigating fraud using Internet technologies is completely absent;

- Lack of ability to use methods of development and version checking;

- Ineffective planning of work related to clarifying the circumstances of fraud through Internet technologies and the production of operational search activities.[80]

The level of investigative work has been growing lately. Many investigators successfully reveal crimes, investigating complex criminal cases. But the majority of investigative officers sometimes erroneously make serious mistakes in carrying out investigative work to investigate theft, using Internet technologies.

Investigatory measures to conduct certain cases are ineffective. The most important circumstances remain unclear. The reason for this is the lack of a clear task for the investigator. The investigator is unable to direct the investigation in the correct direction. The process of investigation is adversely affected by the incorrect use of tactical techniques and the lack of consistency in the actions of the investigator.

[79] Regional Internet registrars / / Materials of the site of the company CISCO. http: //www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-4/regional_internet_registries.html.

[80] Taylor (2015). *Supra nota*. P. 255

Planning, being a method of highly organized investigation, plays an important role in raising the scientific and organizational level and eliminating these shortcomings in the investigation. Employees who are relevant to the practical work, understand planning as the need to draw up an investigation plan. A high scientific and organizational level of investigative work such practice does not provide. It does not contribute to expressing the exact content of the investigation planning.

Drawing up plans for investigating Internet fraud is an expression of planning. It does not give a complete concept of planning. The proper planning required for the effective conduct of Internet fraud investigations is a powerful organizing tool. All employees of the investigative bodies plan to investigate crimes without fail. They ponder every move, the course of the investigation and choose certain actions. Planning involves conducting an accurate organization and a set of specific actions. These actions contribute to the effective identification of the perpetrators of the criminal act and the events themselves related to the crime. The long-standing practice of investigating criminal acts helped to determine the range of actions and their focus.[81] A thorough investigation of practical investigations of crimes proves that, despite the various situations that arise at the very beginning of operational and investigative measures, they can be systematized. This makes it possible to distinguish several separate groups with characteristic, typical features. Do this sorting into groups and means typing.

Relying on all that has been said, it can be concluded that the extent to which operative workers and investigators are correctly handled by the consideration of typical situations depends on how effective the disclosure of Internet fraud will be.

Analyzing such situations, it is possible to send the investigation in the right direction even at the initial stage. This is necessary for the prompt and accurate establishment of truth. Of particular importance is the study of typical investigative situations related to Internet fraud.

It is possible to create and develop certain programs to help the investigator, the main base for which is a set of typical investigative situations. In these programs, it is important to provide guidance and recommendations that are methodical and necessary for the organization and implementation of Internet fraud investigations. A program is needed to carry out certain actions

[81] American Registry for Internet Numbers // Materials of the website of the Internet registrar ARIN. - Access mode: https://www.arin.net/

related to typical investigative situations, a set of necessary recommendations. Such typical situations are typical for different stages of the investigation.[82] Considering typical situations, it is important to take into account the emerging new ways that are used to commit criminal acts, certain traces, methods of criminals, disguise[83]. Separate attention deserves the latest developments and achievements of science and technology, which are useful in carrying out activities to combat the underworld.

But in accordance to previously mentioned developments author would point out a significant arising issue that both investigators and perpetrators do advance in their methods of "work". For that Ajayi E. F. G. states "the efforts made through the instrumentality of legislations at national, international and regional levels were discussed; without prejudice to the effectiveness of the extant laws in place to combat cybercrimes, the scourge persists, nay, rather than the laws to curb, or better still, minimize cybercrimes, there is a rise in the frequency and sophistication and the reason for that development, is attributable to the fact that, as efforts are being made to stem the tide of cybercrimes, so are cybercriminals devising methods and means of thwarting global measures targeted at addressing the problem."[84]

Author's interpretation of Ajayi's statement is that two significant things are pointed out:

1) Cyber-criminals adopt their own measures to enhance their position and make their schemes more complicated.
2) The laws that are adopted to combat cyber-crime have no effect without real law enforcement and punishments.

3.2. The next stage of the investigation of Internet fraud

Investigative situations at the next stage of the investigation of Internet fraud are of great importance. These are programs of action for the investigator, based on typical investigative

[82] Sean Xu (2004). *Supra*.
[83] Disguise methods for internet criminals are mostly the complex digital solutions, or so called "anonymizers" that use Proxi and VPN technologies. Also term "onion routing" can sometimes be used.
[84] Ajayi, E.F.G., Challenges to enforcement of cyber-crimes laws and policy, School of Law, Kenyatta University, Nairobi, 2016, p 4

situations, which are necessary to establish the involvement of the criminal in this crime and to prove his guilt. They need to give guidance and recommendations on the organization and implementation of the investigation of Internet fraud, the production of individual investigative actions in typical investigative situations, to develop a set of relevant recommendations, etc.[85]

During the investigation, it is necessary to identify the most typical situations for Internet fraud that are formed at a later stage. In author’s opinion, it is necessary to take into account new ways of committing Internet fraud, characteristic traces (virtual traces), tricks of criminals, their actions on disguise, as well as the latest achievements of science and technology that can be used in the fight against crime.

On this basis, it is necessary to build private investigation techniques with inclusion of situational versions in them, to give recommendations on planning the investigation of Internet fraud. Inclusion of typical investigative situations in private investigation techniques makes it possible to develop a standard program for investigating Internet fraud.

The first situation is characterized by the fact that there is no data on the identity of the offender who committed Internet fraud. In this investigation situation it is necessary to solve the following tasks: obtaining additional data on the identity of the victim; studying the relationship of the victim with other persons (relatives, friends, co-workers); to check them for involvement in the fraud being investigated.

The investigator must perform the following actions[86]:

- Analyze the initial data obtained at the initial stage of the investigation;
- Identify and question new witnesses; conduct additional (repeated) interrogations of previously questioned witnesses;
- more deeply check the already advanced versions, push and check new versions;
- study similar crimes;

[85] Casey (2014). *Supra nota*. P 202-205
[86] Smith (2001). *Supra nota*. P. 76-85

- to conduct additional questioning of the victim with the involvement of a computer technology specialist; organize listening to telephone conversations;
- to appoint additional and repeated examinations; verify the test on the spot;
- conduct an investigative experiment;
- analyze the way of committing theft; to take a set of measures aimed at finding a criminal (inquiring, monitoring, removing information from technical communication channels, combing the terrain, revealing his connections and circle of contacts, the alleged place of residence, studying the habits and diseases of the offender).

In the following situation, the accused fully admits the blame, his testimony is substantiated by the available evidence. The evidence collected in the case, the confession of the perpetrator of Internet fraud was obtained, and it, as a rule, does not contradict the circumstances of the case. It is necessary to solve the following tasks when conducting investigative actions:

- Collect evidence that confirms the presence of the suspect and the victim at the scene of the incident at a certain time;
- obtain new data confirming the systemic nature of the suspect's actions;
- identify new, additional traces that indicate theft;
- analyze all the information received.

The investigator must perform the following actions:

- interrogation of the accused; additional, repeated interrogations of victims and witnesses;
- presentation for identification;
- identification of new witnesses, an investigative experiment, verification of the testimony on the spot;
- appointment of forensic psychology, forensic psychiatric examination of the accused;
- carry out the scope of investigative actions, which facilitates the consolidation of available information and evidence base.

It is necessary to dwell on errors. For example, the investigator thinks that the information and physical evidence are available in him in sufficient quantity, can be formally taken to conduct the necessary investigative actions to secure them, usually limited to interrogations of interested persons.[87]

In general, difficulties in proving the guilt of specific individuals are related to the fact that the person conducting the investigation may have missed out on the initial stage of the investigation details of the circumstances on the main counts.

The third situation is characterized by the fact that the accused completely denies the facts of committing Internet fraud. The third situation is characterized by the fact that the accused refuses to give evidence.

Tasks:

- to refrain from giving false testimony;
- determine the directions for the search for additional investigative measures;
- evaluate the evidence available in the case;
- search for additional evidence confirming the presence of the suspect and the victim at the scene of the incident at a certain time;
- obtain new data confirming the systemic nature of the suspect's actions;
- Identify new traces that indicate theft committed using Internet technology.[88]

The investigator must perform the following actions: when planning additional questioning of the accused, the investigator (investigator) takes into account such elements as organizational, content and tactical (place, time, number of participants, availability of technical means, determination of circumstances to be clarified, use of tactical interrogation techniques aimed , in particular, on the establishment of psychological contact with the interrogated, etc.); additional, repeated interrogations of victims, witnesses, acquaintances of the accused; presentation for identification of objects; confrontation; investigative experiment; checking the testimony on the spot; appointment of additional examinations (computer-technical and forensic accounting expertise,

[87] Burns (2004). *Supra*.

[88] Tripathi D., Novel Web Fraud Detection Technique using Association Rule Mining, Procedia, Volume 115, 2017, Pages 274–281

forensic, forensic, complex medical and criminalistic, etc.); inquiries, observation, removal of information from technical communication channels, combing the terrain.[89]

In the fourth situation, the defendant confesses his guilt partially. He believes that the evidence put forward by the investigation (inquiry) is unfounded. Therefore, the defendant's interest in concealing the facts of his criminal activities before the investigation (inquiry) is obvious.[90]

In this situation, the investigator (investigator) needs to focus on the following tasks:

- to overcome the attempt to give false testimony; prepare for conflicting and negative behavior of these persons during interrogation;

- determine the directions for the search for additional investigative actions;

- evaluate the evidence available in the case;

- search for additional evidence confirming the presence of the suspect and the victim at the scene of the incident at a certain time;

- obtain new data confirming the systemic nature of the suspect's actions;

- Identify new traces that indicate theft using Internet technologies.

In the fifth situation, the offender is recognized in Internet fraud, but is not recognized in other crimes (extortion and other components of 2% of cases).

In this situation, the investigator needs to focus on the following tasks:

- to overcome the attempt to give false testimony;

- Prepare to overcome the negative behavior of these individuals during the interrogation;

- determine the directions for the search for additional investigative measures; assess the evidence available in the case;

[89] Атаманов (2012). *Supra*.
[90] Fischer (2007). *Supra*.

• search for additional evidence confirming the presence of the suspect and the victim at the scene of the incident at a certain time;

• obtain new data confirming the systemic nature of the suspect's actions;

• Identify new traces that indicate theft committed using Internet technology.

Algorithm of the investigator's actions: repeated deep examination of witnesses (since previously unknown episodes of other crimes, as well as additional thefts, are known from their words); identification of additional witnesses; interrogation of the accused, interrogation of witnesses established after a certain period of time after the commission of the crime; repeated questioning of witnesses interrogated at the initial stage of the investigation of theft; conducting face-to-face bets, an investigative experiment, checking the testimony on the spot; appointment of additional forensic medical examinations; presentation for identification of objects; confrontation; investigative experiment; checking the testimony on the spot; appointment of additional examinations (computer-technical and forensic accounting expertise, forensic, forensic, complex medical and criminalistic, etc.); inquiry, observation, removal of information from technical communication channels.[91]

As pointed out previously analysis of criminal cases on Internet fraud related to this situation shows that the behavior of a criminal at the time of his interrogation can develop in three areas:

- Firstly, the accused, denying guilt, himself sets out the picture of the event;
- Secondly, in his testimony the offender refers to an alibi;
- Thirdly, he is silent, completely refusing to give testimony using right against self-incrimination. The work of the investigator should be aimed at a thorough analysis of the evidence gathered in the case. Then, to identify witnesses characterizing the identity of the accused; the establishment of employees (colleagues) who could give testimony on the fact that the victim applied for help.

The investigator checks the alibi put forward by the perpetrator, as much as possible detailing his testimony. At the same time, the investigator should work closely with the criminal investigation detective, the precinct officers, in order to obtain additional evidentiary information, indicating the

[91] Gregg (2006). *Supra*.

person's involvement in the committed act (committing the same cases to the perpetrators). This is due to the fact that the majority of the accused are aware of the increasing degree of criminal responsibility, depending on the number of episodes of criminal activity. Therefore, during the interrogation, they try to keep silent about unidentified or unproved episodes.[92]

While confessing in the commission of the episodes of criminal activity established by the investigation at the time of the accusation and denying the existence of others, the accused of fraud is justifiable, from his point of view, he hopes for the imposition of punishment by the court not connected with deprivation of liberty.

It should be noted that the accused of embezzlement, admitted during the interrogation in the commission of additional facts of the hacker attack and who rendered significant assistance to the investigation, make up less than 2% as mentioned previously.

In other cases, these individuals denied the obvious facts or gave false testimony about the time and place of stay. Only in the presence of conclusive evidence recognized additional episodes of the criminal act. Of great importance for the investigation of Internet fraud is the conduct of a complex of investigative actions (inspection of the scene, computer device, interrogation of witnesses, appointment of examinations), during which it is possible to obtain data confirming the facts indicated to the injured. The investigator, having compared the information, having correctly constructed the interrogation of the accused, has a chance to fully expose him in committing a crime.[93]

Thus, each of the investigative situations arising at the subsequent stage of the investigation of Internet fraud, corresponds to its tasks and programs of action of the investigator. One more important issue when organizing the investigation is the right determination of perpetration according the local penalty law. For example in Estonian Penalty Code[94] there are different compositions of perpetration like §209 “Scam” and § 213 “Computer Scam”. The particular difference is, if the damage to the victim is caused by knowingly creating an incorrect understanding of the actual facts (for example wrong information on product in online auction, etc) or by the unauthorized insertion, modification, deletion, infringement, blocking or otherwise

[92] Bignell, K.B., Authentication in an Internet Banking Environment; Towards Developing a Strategy for Fraud Detection. ICISP 2006, p. 23.
[93] Chang (2008). *Supra*.
[94] KarS, RT I, 30.12.2017, 29

of the computer program or data by unlawful interference with the processing of the data.[95] In author's opinion with such distinction not much border cases can occur, but there are other compositions of crimes related to § 213, like § 206 “Interference with computer data” and §207 “Preventing the functioning of the computer system”, therefore bordering and determination of these cases are left to the court.

3.3. The content and the features of collecting evidence on criminal cases of Internet fraud

Collection of evidence in the investigation of criminal cases of fraud committed using the Internet is a prerequisite that is inherent in all criminal cases. It is evidence that is the main element in the system of proof within the legal framework. Particular attention among the ways to obtain evidence in this thesis work we will address the requests.

A tactically well-formed query greatly facilitates the investigation of fraud committed using the Internet, and the information obtained is evidence in the case. Under a tactically well-formed request is meant promptly directed to state authorities, enterprises, institutions and organizations, officials and individuals possessing information that is of interest to the investigation, and having the opportunity to provide it in the manner prescribed by law, a request in which all are displayed necessary circumstances to be determined at the time of its dispatch.

Based on the technical features of the process of transmitting information on the Internet, the timeliness of sending the request is that:

- in the shortest possible time a decision is made on the need to send a request, the question of who should address it is decided, a list of necessary circumstances to be covered in the response to the request is determined, on the basis of which a list of issues is formulated;

- it is taken into account that the response requires a period of time, depending on: a) the amount of data that must be set to provide a complete response; b) the availability and the way of

[95] Pikamäe, P., *Karistusseadustiku kommenteeritud väljaanne*. Juura kirjastus, Tallinn, 2015, § 206-213

storing the requested information; c) geographical location of the addressee; d) the manner in which the request / response is transmitted – statutory order.

In author’s opinion, further use of the information received in response to a request as evidence should be considered legitimate and consider such an answer as a document. The circumstances that need to be set by the request[96]. When investigating a criminal case of fraud in an online auction or an online store, a request is made to the administration of the service, which states:

1) how the fact (s) of fraud (message from users of the service, own monitoring, the appeal of law enforcement bodies, etc.) was established (s):

- when communicating from users: a) the list of users from whom the complaints were received, the time of their receipt (including registration data: name, surname, patronymic, contact information: e-mail, telephones, etc.); b) a brief summary of the substance of the reports of the offense (poor quality or non-conformity of the goods, non-appearance of the goods, etc.); c) information about the goods (lot), which is the direct object of the conflict situation (available photos, description given, time for sale); d) the time when the sale agreement (s) was concluded (s) (time of expiration);

- with self-identification (monitoring): a) a list of users who were identified as victims (including registration data, contact information, etc.); b) the essence of the detected violation; c) information about the goods (lot) (photos available, description given, time of putting up for sale, IP address from which the lot was exhibited); d) the time when the sale agreement (s) (or) the time (s) of the sale (s) have been concluded; e) circumstances that served as grounds for suspecting the unfair conduct of one of the parties;

2) how the Internet auction is carried out. In this case, rules are requested regarding: a) the operation of the service; b) registration and activation of the account on the site; c) conclusion of purchase-sale agreements (requirements for lots, information about them, etc.); 3) provide available information on activities of the fraudster: a) registration information (exact date and time), as well as the method of identity confirmation; b) whether it is a legal entity or an individual (firm, private entrepreneur, etc.); c) goods (lots) for sale; d) information regarding buyers (winners

[96] For example see UK Information Commissioner’s Office explanation at: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/receiving-a-request/

of trades), persons suspected of fraud; e) information on other bidders on a particular lot that has become the direct object of fraud; f) the history of visits to the site (time of entry and location, IP addresses for which the site was visited); g) whether there are other accounts that belong to this user, if there is, then provide the above information on them; h) information regarding the blocking of user accounts, timing and reasons for blocking; i) existing complaints about user accounts (if necessary - attach screenshots); j) correspondence between the fraudster and the victim (s) (if any); l) was the damage caused directly to the Internet auction (online store), if so, which one. The issue of fraud in an online auction or online store can be confirmed by information from a service that carried goods from the seller to the buyer. The request to the service that was engaged in the transportation of goods can determine the fact of receipt or non-receipt of goods by the party and obtain information on the characteristics of the goods (dimensions, weight, etc.).

In the request, you should note such data as: 1) the date of shipment; 2) the characteristics of the cargo (weight, dimensions, special requirements for transportation, etc.); 3) who carried out the dispatch (if possible, the surname, name, patronymic and information on the documents that were provided for the verification of identity - type of document, series, number, etc.); 4) from what address and to what address the transportation was issued; 5) the payee's records, which were indicated by the sender; 6) the date of arrival of the goods at the specified address; 7) a method for informing the consignee of the arrival of the goods; 8) the date of receipt of the goods (if such a fact took place); 9) information about the person of the recipient (if possible, surname, first name, patronymic and information on the documents that were provided to verify the identity - type of document, series, number, etc.); 10) the availability of documents that certify the fact of receipt (invoice with the signature of the recipient, a receipt journal, etc.).[97]

In the event that the fraud is committed in a way that involves activities directly on the resource (site, social network, etc.), to obtain information that may be of interest to the investigation, it is necessary to send a request to the administration of the resource on which fraud was committed. At the same time, it should be noted that the request must include the login (nickname) of the user, the information that the investigator needs to receive, as well as the maximum concretization of the time of his activity on the resource that the investigation is interested in.

[97] Boyer, M. M., Centralizing Insurance Fraud Investigation, Geneva Papers on Risk and Insurance Theory, Vol. 25:2, 2000, 159-178.

To the mandatory circumstances that must be displayed in the request, we refer to:

1) registration data entered by the user when registering on the resource;

2) date, time of registration and IP-address of the user at registration;

3) IP address of the user in the specified period of time.[98]

We consider useful information that can be provided by providers of Internet connection services (providers). In carrying out the research, we decided on the issue of the possibility of establishing a particular person (name, first name, patronymic, place of residence, etc.) in the presence of the IP address from which the crime was committed.

It is known that the range of IP addresses that can be used to assign nodes to public nodes is exhaustive. Organizations dealing with the distribution of IP addresses are regional Internet registrars.

For today, five regional Internet registrars are singling out:

1) American Registry for Internet Numbers[99];

2) RIPE Network Coordination Center[100];

3) Asia-Pacific Network Information Center[101];

4) Latin American and Caribbean Internet Addresses Registry[102];

5) African Network Information Center[103].

The status of a regional Internet registrar can only be assigned to ICANN. All these regional Internet registrars operate with certain amounts of Internet resources that are delegated to them by the American non-profit organization IANA.

[98] Staples (2008). Surpa nota. p 163.

[99] See more at: https://www.arin.net/

[100] See more at: https://www.ripe.net/

[101] See more at: https://www.apnic.net/

[102] See more at: http://www.lacnic.net/web/lacnic/inicio

[103] See more at: https://www.afrinic.net/

Having examined the principle of the subordination and distribution of the IP address space between the providers of the Internet connection service, author, among other things, singled out one forensically significant circumstance: in order for the local level provider to be able to provide services for connecting to the Internet to the end user, it must be registered with its regional Internet registrar in accordance with the specified regions. This circumstance greatly simplifies the search for a local level provider providing the service to the person who is wanted.

In particular, after studying the RIPE Network Coordination Center site (http://www.ripe.net/), it was found that it can receive information on the provider that provides the service of connecting to the Internet in the presence of an IP address of an unidentified person. To do this, it is enough to use the search in the database of the regional Internet registrar by entering in the search line a well-known IP address in point-and-tithe form, and start the search.

The search results display information about the local ISP. This information greatly simplifies the search for a service provider, because it is characterized by a high level of information about the searched object.

It is understood that the use of information obtained in this way as evidence in a criminal case is inadmissible. However, using it as an orientation tool will significantly speed up the investigation and significantly improve its quality.

In terms of evidence, the official response to a request received from an Internet registrar can be proof.[104] However, such a response will have to wait a long time. To accelerate the necessary operations, you can use electronic document flow: the request is sent to the official e-mail of the regional Internet registrar, the response is also received by e-mail.

Further it is recommended to address with the request to the provider, information about which was received in the above manner. The request states:

1) since when the provider is engaged in the provision of Internet connection services;

2) what range of public IP-addresses the provider rents for the provision of its services;

3) whether the specified IP-address (or several) is included in this range;

[104] Carter, D.L., Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies, School of Criminal Justice Michigan State University, 2nd edition, 2009 P. 59

4) how the public IP address is issued to customers;

5) whether the provider uses local IP addresses and how they are assigned to the client when connected;

6) what authentication system is used by the provider;

5) which of the users received the specified IP-address (in view of time intervals) as public.

In this case, as the IP address and the corresponding time of their use, those that are received during the investigation (for example, in the response of the service on which the crime was committed) are indicated.[105]

In the request it is necessary to specify the data of greatest interest: a) surname, name, patronymic; b) date of birth; c) address of residence; d) number, series of passport and identification number (possibly, were received at the conclusion of the contract); e) information on the method of user authentication: login, MAC address; e) information on the number of connected devices or the use of routers (if such is owned by the provider); g) copies of documents on the provision of services (in particular, the agreement with the annexes).

In the case when a public IP-address was rented by several users during the specified period, it is necessary to provide the specified information regarding each.

The features of information obtained by the investigator during the investigation of fraud committed using the Internet allow us to obtain information about: a) the technical nature of the crime committed; b) the amount of damage, as well as the person to whom it was caused; c) the technical identifiers of the devices used to access Internet resources in the commission of a crime (IP address, MAC address); d) indirectly (and in some cases directly) to obtain information about the person who committed this crime.

However, effective gathering evidence does not mean the effective prosecution process. While there are countries which have no substantive or procedural laws against cybercrime cases then

[105] Taylor (2015). *Supra nota*. P 278-301

the offenders might pass away from criminal prosecution like with “I love you” virus[106]. In authors opinion similar cases are likely to be evaluated like violation of law principle *aut dedere aut judicare,* nevertheless there is no effective mechanism to avoid them if the local legislature of a country has not adopted laws against cyber-crime.

Ajayi states in his article[107], that “According to the United Nations, 32 there are 193 Full UN Members, 2 Observer States and 6 States with partial recognition, making a total of 201 countries in the world. Out of this number, only about 79 countries (Ajayi, 2015), the majority being in Western Europe comprising 47 countries, have laws specifically enacted for cybercrimes; a simple inference that could be drawn from above data is that less than 40% of countries in the world have laws forbidding cybercrime.” According to Ajayi such situation is giving cybercriminals a license to operate freely without fear but rather with impunity. He also points out, that only four countries on African continent have legislation against cyber-crime, namely Cameroun, Kenya, South Africa and Zambia.[108]

The situation is likely to be resolved in natural evolution of legislation, when countries take over and adopt the effectively working regulations. “Soft Law”, recommendations, and exchange of experience are in author’s opinion the best ways to improve the situation.

Also the problem of computer data access arises. According to Cristos Velasco “it should be borne in mind that a large part of the evidence needed in criminal proceedings is hosted and preserved in different servers located and hosted in the cloud by Internet companies like Yahoo, Google, Microsoft, Skype and social networks like Facebook and Twitter, which established their own methodologies, criteria and cooperation procedures in order to disclose information and data to law enforcement authorities for identification of possible suspects” [109]. Therefore there is always a risk that the hosting company can decline the inquiry, if there is a conflict of legal rulings. Even if the court considers the case in favor of investigator[110], and force the Internet company to issue data, the valuable time for effective investigation will be lost.

[106] Virus created by two programmers from Philippines that affected millions of computers worldwide in year 2000. Philippines did not have a regulation in the criminal law concerning creation and dissemination of viruses at that time, so the prosecutor dropped all the charges.

[107] Ajayi (2016). *Supra*.

[108] *Ibid*

[109] Velasco, C., Cybercrime jurisdiction: past, present and future, ERA Forum, 2015

[110] For example Yahoo v Belgium, or Microsoft corp v USA cases

Currently there are multiple international regulations to make computer data accessible by the investigator, among which there are Regulation (EU) 2016/794[111] settling rules for data access and exchange between Europol and member states institutions or private persons. The scheme of cooperation foresees that Europol is gathering and providing data through its local departments, which build cooperation with local investigative agencies and private persons in cases foreseen in article 27. In general cases local investigative agencies are the ones to gather evidence and provide it to Europol.

However, because of the volatility of digital evidence, or because of the risk of their being destroyed quickly, these measures may not provide sufficient access to data. The mechanism of mutual legal assistance, which may take some time to answer a letter of access to legal aid, has been subject to criticism.[112]

If we observe Estonia as an example, then KrMS §117 and §118 are the norms that the investigator is using when making inquiries concerning data mentioned previously, that may be the proof of perpetration.[113] The data gathered for evidence can be provided to another EU member investigative agency through Europol according to the Regulation (EU) 2016/794 or directly to another countries government using KrMS §473.[114] The last one is from authors point of view is more time-efficient investigative cooperation way.

Also it is important to point out, that according to KrMS § 3 Estonia can make proceedings against its own citizens no matter if they are in Estonia or are outside. It means, that if the suspect is Estonian citizen, and data from suspect's computer is obtainable by use of the internet, then the investigator can obtain it directly. There is no unified position on the question if it will be considered a cross-border investigative activity or not, as it came out from research made by A.-M. Osula.[115] Which means, that there is no supreme regulation for that. Therefore this issue can be a subject for a separate study, which stays out of borders for current thesis.

[111] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

[112] Osula, A.-M., Täidesaatev jurisdiktsioon ja piiriülene kaugläbiotsimine, Juridica, No. 2017/8, 2017, 559-566

[113] Kergandberg, Eerik,. Kriminaalmenetluse seadustik, Kommenteeritud väljaanne. Juura, 2012, p 319-323

[114] Kergandberg, E., (2012). P. 1044

[115] Osula, A.-M. (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. – *International Journal of Law and Information Technology, Vol.* 24, No. 4, 356–371.

On the above author concludes the current problem when investigator is trying to reach the technical identifiers is standing behind purely technological issues in case if the perpetrator is using disguise technologies.[116] In favor of such conclusion also speaks G. Horsman's study[117], who states that as cyber-criminals also develop technologies of perpetration and start using top-level disguise technologies, then at some point the law enforcement agencies can be unable to combat cyber-crimes due to lack of technological opportunities. The Horsman's idea is partially supported by the recent study of S. Adee, who claims, that to combat cyber-crime better law enforcement is needed rather than new laws.[118] Adee's point of view is supported by the researched of Velasco[119] who find, that currently there are sufficient domestic and international regulations.

[116] See page 43

[117] Horsman, G., Can we continue to effectively police digital crime? - *Science & Justice*, Vol. 57, No. 6., 2017, p 448-454.

[118] Adee, S., The online arm of the law. New Scientist, Vol. 237, Issue 3171. 2018, p22-23.

[119] Velasco (2015). *Supra*

3.4. Methods on Prevention of internet fraud

An easy measure to prevent internet fraud is suspending the digital services by the service provider in case of suspicious transactions taking place. For example the banks in their client agreement terms foresee that they are free to shut down credit cards in case if behavior unusual[120] for card user takes place, or in case if transactions are made to entities placed in high-risk regions[121]. The risk of such measure is defined by a possibility that a client will have no access to the bank services and can be left without money for no specific reason just due to a risk, that the suspicious transaction can be fraud. Such situations frequently occur with credit card users when being on a trip to Asian or African region, where the statistical risk of fraud is higher.[122]

Although suspension of services is questionable from the position of Law of Obligations, because the service provider does not provide the agreed service, which can possibly bring damage to the client, and also can be qualified as discrimination by businesses in high-risk regions, it remains very effective. In authors opinion its effectiveness is due to short time of response to the threat, and also not having any obligations to gather high-quality straight evidence of fraud.

It is necessary to point out, that suspension of digital services, as an action against internet fraud in particular and cyber-crime in overall, is widely used by the governments of some countries. For example China Cyber-Security services suspends hundreds of websites, smartphone applications and mobile network services for the means of national security.[123]

Also Russia has recently been standing out as an active digital service suspender. In the recent year Russian courts have recognized illegal websites of 11 non-profit organizations among which: The National Endowment for Democracy, Open Society Foundation, U.S. Russia Foundation for

[120] Clients behavior is nowadays tracked automatically, and suspicious transactions have to be reconfirmed by the bank representative. For reconfirmation the service provider usually contacts the client, and check the details of the transaction.

[121] For example see Swedbank credit card agreement paragraph 3.10, 3.11 and 4.3

[122] See Swedbank Policy

[123] Lindsay Jon R, China and Cybersecurity, Oxford University Press, Academic division, 2015, pp 55, 71-77, 315-330

Economic Advancement and the Rule of Law, etc. [124] And also Telegram messenger, which is widely used by younger generation of businessman due to its highly effective encryption, was also suspended under a resolution of court.[125] [126]

Considering the above mentioned one can see that Russian website and internet service blocking is generally made according to the point of view of the national security, or related institutions. Researching the court decisions on website blocking initiated by private individuals or private legal entities author could not find a suitable case, where a website would be blocked due violation of private law terms. This clearly shows that a country has “prioritized” some particular cases in front of others.

Great Britain on the contrary has significantly different approach to the issue of blocking websites used unlawfully. The example for it is the recent case Cartier v BSkyB, where Richmont – the proprietor of Cartier, Mont Blanc and IWC trademarks, sought orders against five main internet service providers (ISPs), Sky, BT, EE, TalkTalk and Virgin (collectively holding 95 per cent of the UK broadband market), claiming they had to block access to websites involved in selling counterfeit goods.[127] The legal dispute arose from the question if the court had jurisdiction to make such an order pursuant. Here the court finds that the court had jurisdiction to make such an order pursuant according to s.37 (1) of the Senior Courts Act 1981.[128] However, there is a dissenting judgement from Briggs LJ who believed that the costs of implementing the blocking order should be borne by the right holder making the application, because it goes against the underlying principle in equity if the innocent party has carrying the burden of costs of such actions.[129]

The above mentioned case resolution is believed to be a new powerful weapon for British claimants against ISPs in their demands to block sites and suspend internet services. But it also

[124] BBC Russia, 11 "друзей" Роскомнадзора: какие сайты запретили в России, 12.12.2017 (https://www.bbc.com/russian/news-42324276)

[125] Таганский Районный Суд Москвы, 02-1779/2018, 13.04.2018

[126] Firstly Telegram Messenger LLP was punished with a fine 800 000 RUB, for not disclosing the encryption algorithms to Russian federal security service FSB by the Meschanskiy Court of Moscow (case number 5-1794/2017, resolution made on 16.10.2017), and after continuously non-disclosing the encryption algorithms organization Roskomnadzor demanded the Telergam Messenger services to be blocked.

[127] Blythe A., Black markets, grey markets and online marketplaces: attempting to prevent the sale of trade mark infringing goods online post-Cartier v B Sky B, E.I.P.R. 2017, 39(5), 279-285

[128] United Kingdom Supreme Court decision, 30.01.2018, UKSC 2016/0159

[129] Blythe (2017). *Supra*.

shows the different approach to the usage of blocking possibilities compared to Russia and Eastern Asia, where according to the available court practice only governmental institutions have initiated the blocking website or internet service.

In authors opinion Cartier v BskyB case resolution is notable for other EU countries, and is worth being adopted to EU regulations concerning ISPs, but at the same time it contains risks, that if ISPs, willing to minimize the costs they have to bare, will start permanently blocking all suspicious sites. That can be on one hand interpreted as violation of freedom of entrepreneurship, and on other hand it can become discriminative for businesses from “high-risk” areas. This issue deviates from the main objective of current paper, therefore it can be a matter for another research.

In Estonia, for instance, there are multiple regulations allowing the government to block sites and suspend digital services under deferent laws. For example a fraudulent pyramid investment scheme MMM2012[130] was suspended by blocking two of organization sites by Tax and Toll department of Estonia (MTA) under HasMS[131] §55 and §56. The named pyramid scheme was considered illegal gambling, and norms that are foreseen to defend the players against illegal gambling were used accordingly. Unfortunately there is no ruling, if such classification of pyramid schemes is right or wrong because MMM2012 did not take MTA to the court with a claim.

In authors opinion it is a great advantage of Estonian law, that law enforcement authorities can block sites and suspend internet services and other digital services without the court’s decision, but based purely on suspect of perpetration. It gives Estonian law enforcement and investigative agencies a strong predominance to use preventive actions on internet fraud.

As a result of the research made author concludes that Estonia law enforcement has powerful instruments to prevent internet fraud, but weak investigative capability for such perpetration. Therefore it is necessary to develop competence of investigative agencies to react on perpetrations that already took place.

[130] See more at: https://www.aripaev.ee/uudised/2012/10/09/uus-puramiidskeem-hullutab

[131] HasMS, RT I, 25.04.2012, 1 (valid until 05.06.2012)

CONCLUSION

Summing up, it should be said that our work, taking into account its goals and objectives, made it possible to identify a number of theoretical and practical issues and problems facing law enforcement officials in the process of identifying, uncovering, investigating and preventing Internet fraud. The research make it possible to draw the following conclusions.

Based on modern achievements of criminalistics as a science and analysis of leading judicial and investigative practices, we have identified the content of elements of forensic features of Internet fraud, revealed the existing patterns between them. The structure of forensic features of Internet fraud includes the following elements: conditions for the commission of criminal acts, methods and motives of offenses, characteristic traces of crimes, information about the identity of the offender, data on the identity of the victim.

The peculiarity of the mechanism of trace formation in the commission of crimes of this category is that the formation of virtual tracks is based on a specific electronic-digital mapping occurring in a computer system and (or) virtual space (cyberspace). Recognition of the place of committing cybercrime is impossible without establishing an environment for the commission of a crime, which is determined by the cyberspace system.

To investigate crimes committed in cyberspace, both technical and theoretical knowledge are required. Therefore, there is a need to develop a single concept of cyberspace in terms of forensic science. Cyberspace is the area of interaction of systems of various levels, including the following elements: computer, computer systems, networks (both global and local), computer programs of users, as well as data circulating in the listed elements.

As a result of the research made, the author’s opinion is that the problem of internet fraud is possessed by the fact, that investigative agencies mostly lack knowledge and competence in the sphere of digital technologies, therefore are not able to respond adequately on the threat coming from fraudulent use of digital technologies. Observing the example of Estonia and its investigative agencies like Police, Tax and Toll Board, Consumer Protection Department etc – non of them have the defined strategy on staff training in digital fraud area, therefore their methods of investigation are outdated, and not ready to face the modern technological challenges. There are relevant laws and international legislation that help identify the internet fraud and register the case, but the law enforcement mechanisms and investigation methods are insufficient for perpetrations that already happened.

Internet fraud prevention, on the contrary, in Estonia has well organized mechanism because law enforcement can suspend and block websites and use other suspension instruments without court decision, which helps to minimize the risks of emerging of big fraudulent schemes.

A successful investigation of Internet fraud in many ways depends on the initial information that is available to the investigator at the beginning of the investigation. One of such information bases can be considered a forensic classification. The criminalistic classification of crimes is also oriented towards active practical application in the course of investigative activities, contributes to a proper understanding of the essence of the events under investigation, the competent construction, selection and application of criminalistic techniques for the investigation of certain types of fraud.

The questions studied and solved in the thesis work give rise to new scientific problems, among which:

1. Organization of a system for regulating legal relations in virtual economies and protecting the rights and legitimate interests of participants in these legal relationships.

2. Adapting the accumulated experience and knowledge about the investigation of traditional crimes to the modern needs of law enforcement agencies to investigate crimes committed on the Internet.

3. Analysis of the application of the rules of law in the investigation of Internet fraud and other high-tech crimes in order to improve legislation, above all, on law enforcement.

4. Further development of new effective methods for preventing Internet crime.

5. Development of the most effective schemes for interaction between law enforcement agencies and victims in order to achieve the greatest confidence in the investigation of crimes (especially if the victim is a large legal entity).

As can be seen, not all of these tasks are resolved by criminal law. Therefore, the submitted research paper will be of interest not only for criminal lawyers, but also for researchers in such areas as civil law, economics, criminal law, criminal procedure and norm-setting activities.

In addition, speaking of criminalistics, it should be noted that the questions posed in this thesis need further study. Since Internet crime is developing extremely quickly, it is important to continue to study the problems of the methodology for investigating Internet fraud in order to accumulate new and update knowledge obtained in other studies on this topic.

The scientific research carried out in the thesis made it possible to draw a number of conclusions.

1. Fraud in the Internet has a number of differences compared to traditional fraud. These differences determine the specifics of the investigation of this crime. In particular, such features are manifested in the bordering and defining of right composition of perpetration, production of operational-search activities and investigative actions.

2. The conduct of operational search activities and investigative actions in the investigation of Internet fraud is complicated by the fact that some of the information produced during their production is extracted from sources of virtual information (computer of the victim or criminal, remote local server, Internet, etc.) and is highly volatile and can be destroyed during the time investigator spends waiting for bureaucratic issues to be resolved.

3. On the basis of the material studied, recommendations are made to the investigators on the production of certain operational and investigative measures and investigative actions, which are of particular importance and complexity for the investigation of Internet fraud.

Also, depending on the method of commission of the crime, recommendations are given to compile a list of issues that are advisable to ask the victim and the accused or suspect during interrogation.

In the theory and practice of responding to incidents of information security at enterprises, the high importance of such a stage as the analysis of the conducted investigation with the purpose of increasing the effectiveness of the actions of the subjects of investigation in the future, as well as the development of measures to prevent new incidents, is noted. It seems that a similar event will bring tangible benefits to law enforcement officers involved in the investigation of high-tech crimes. Like traditional fraud, Internet fraud is characterized by high dynamism in terms of ways to commit. Therefore, it is extremely important to discuss the most difficult moments in the investigation. Implementation of this recommendation will improve the level of theoretical and practical training of investigators due to more rapid development of new knowledge.

Due to the relevance of the topic, the results of this work should contribute to the further study of Internet fraud, as well as other crimes committed on the Internet. The main conclusions and recommendations of the study can be used not only by theoretical researchers, but also by practitioners to improve the practice of investigating crimes.

20715 words

LIST OF REFERENCES

Scientific books

1. Casey E. (2014). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* 3rd ed. London: Elsevier.
2. Carter, D. L., Ph.D., (2009). *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2nd ed. East lansing: School of Criminal Justice, Michigan State University.
3. *Intelligence and Security Informatics. First NSF/NIJ Symposium, ISI 2003, Tucson, AZ, USA, June 2-3, 2003, Proceedings* (2003). Eds. H. Chen, R. Miranda, D. D. Zeng, C. Demchak, J. Schroeder, T. Madhusudan. 1st ed. Berlin: Springer.
4. Jaishankar, K., (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* 1st ed. Abingdon: CRC press.
5. Hecker, B., (2010). *Europaisches Strafrecht.* Berlin: Springer.
6. Kergandberg, E., Pikamäe, P., (2012). *Kriminaalmenetluse seadustik, Kommenteeritud väljaanne.* Tallinn: Juura kirjastus.
7. Kranacher M.J., Riley R., Wells J.T. (2012). *Forensic Accounting and Fraud Examination.* Chishester: John Wiley & Sons Ltd.
8. Lindsay J.R., Cheung T.M., Reveron D.S., (2015). *China and Cybersecurity.* Oxford: Oxford University Press.
9. Pikamäe, P., Sootak, J. (2015). *Karistusseadustiku kommenteeritud väljaanne*. Tallinn: Juura kirjastus
10. Riordan J., (2016). *The Liability of Internet Intermediaries.* Oxford: Oxford University Press.
11. Staples, H., (2008). *The legal status of third country nationals resident in the European Union / Staples Helen II European monographs*. Cambridge: Kluwer Law International.

12. Taylor R.W., Fritsch E.J., Liederbach J., (2015). *Digital Crime and Digital Terrorism*. 3rd edition. London: Pearson.
13. Turvey, B. E. (2014), *Forensic Victimology*. 2nd edition. Oxford: Elsevier Inc.

Scientific articles:

14. Adee, S. (2018). The online arm of the law. - *New Scientist*, Vol. 237, Is 3171. 22-23
15. Ajayi, E.F.G. (2016), Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, Vol. 6, No. 1, 1-12
16. Albert Miriam R. (2002). E-buyer beware: why online auction fraud should be regulated. - *American Business Law Journal*, Vol.39, No. 4. American Business Law Association. 575-644.
17. Gavish B., Tucci C.L. (2008). Reducing internet auction fraud. - *Communications of the ACM*, Vol. 51 No. 5, Pages 89-97
18. Bignell, K.B. (2006). Authentication in an Internet Banking Environment: Towards Developing a Strategy for Fraud Detection. - *International Conference on Internet Surveillance and Protection (ICISP).* 26-29 August 2006, Cote d'Azur. IEEE, 23-30.
19. Blythe, A. (2017) Black markets, grey markets and online marketplaces: attempting to prevent the sale of trademark infringing goods online post-Cartier v B Sky B. - *European Intellectual Property Review*. Vol 39, No. 5, 279-285
20. Boyer, M. M. (2000). Centralizing Insurance Fraud Investigation. *Geneva Papers on Risk and Insurance Theory*, Vol. 25:2 159-178.
21. Burns Ronald G., Whitworth Keith H., Thompson Carol Y. (2004). Assessing law enforcement preparedness to address Internet fraud. - *Journal of Criminal Justice*. Vol. 32, No.5, 477-493.
22. Chang, Joshua J.S., (2008). An analysis of advance fee fraud on the internet. - *Journal of Financial Crime*. Vol. 15, No. 1, 71-81,
23. Chiemeke, S. C., Evwiekpaefe, A. E. 2006. The Adoption of Internet Banking in Nigeria: An Empirical Investigation. - *Journal of Internet Banking and Commerce*. Vol. 11, No. 3.
24. Chua, C.E.H., Wareham J. (2004). Fighting Internet auction fraud: an assessment and proposal. - *IEEE Computers*. Vol. 37, No. 10, 31-37.

25. Elkind, E. (2008). Varavastane süütegu Interneti keskkonnas: selle piiritlemise probleemid Eesti karistusõiguses. – *Juridica,* No. 2008/5. 333-337.
26. Fischer, M., Gordon, T., Greenlee, J., Keating, E. (2007). An Investigation of Fraud in Nonprofit Organizations: Occurrences and Deterrents. - *Nonprofit and Voluntary Sector Quarterly*, Vol. 36, No. 4, 676-694
27. Grazioli S., Jarvenpaa S.L. (2000). Perils of Internet fraud: an empirical investigation of deception and trust with experienced Internet consumers. - *IEEE Transactions on systems, man and cybernetics,* Vol. 30, No. 4, 395- 410
28. Gregg, Dawn G. (2006). The Role of Reputation Systems in Reducing OnLine Auction Fraud. - *International Journal of Electronic Commerce*, Vol. 10, No. 3, 95-120.
29. Helberger, N., Loos, M. B. M., Guibault, L., Mak, C., Pessers L, (2012). Digital Content Contracts for Consumers: Digital Content Contracts for Consumers. – *Journal of Consumer Policy,* Vol. 36, No. 1, 3.
30. Herlin-Karnell, E. (2012). White-Collar Crime and European Financial Crises: Getting Tough on EU Market Abuse. – *European Law Review*, No.2012/4, 481–494
31. Hirskin, E. (2014). Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid. - *Juridica*, 2014/8, 611-624
32. Horsman, G. (2017). Can we continue to effectively police digital crime? - *Science & Justice,* Vol. 57, No. 6. 448-454
33. Longe O., Osofisan A. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. -*The African Journal of Information Systems*, Vol. 3, No. 1. 16-26.
34. Moreno-Fernandez, M., Blanco F., Garaizar P., Matute H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. -*Computers in Human Behavior*, Vol 69, 421-436.
35. Nimmo, Merika, (2017). Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis. - *Juridica* 2017/10, 710-717.
36. Olmstead K., Smith A. (2017). Americans and Cybersecurity. Washington DC: Pew Research Center.
37. Osula, A.-M. (2016). Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study. – *International Journal of Law and Information Technology, Vol.* 24, No. 4, 356–371.

38. Osula, A.-M. (2017). Täidesaatev jurisdiktsioon ja piiriülene kaugläbiotsimine. - *Juridica*, No. 2017/8, 559-566
39. Pratt T. C., Holtfreter K., Reisig M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. - *Journal of Research in Crime and Delinquency,* vol. 47, 267-296.
40. Sean Xu. (2004). Global Technology, Local Adoption: A Cross-Country Investigation of Internet Adoption by Companies in the United States and China, - *Journal of Electronic Markets,* Vol. 14, No. 1, 13-24.
41. Smith Russell G., Urbas Gregor, (2001). Controlling Fraud on the Internet: A CAPA Perspectiv: a report for the Confederation of Asian and Pacific Accountants. - *Research and public policy series.* No. 39. Canberra: Australian Institute of Criminology.
42. Tripathi, D., Nigam, B., Edla, D. R., (2017), Novel Web Fraud Detection Technique using Association Rule Mining, - *Procedia,* Vol. 115, 274–281.
43. Velasco, C., (2015). Cybercrime jurisdiction: past, present and future. - *ERA Forum - Journal of the Academy of European Law Springer.* Vol. 16, No. 3, 331-347.
44. Wright R. T. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. - *Journal of Management Information Systems*, Vol. 27, No. 1. 273-303.
45. Атаманов, Руслан Сергеевич, (2012). Основы методики расследования мошенничества в сети Интернет, Московская государственная юридическая академия, Кандидатская диссертация, Москва
46. Комаров А.А, (2011), Криминологические аспекты мошенничества в глобальной сети Интернет, Саратовская государственная академия права, Кандидатская диссертация, Саратов
47. Тарасенко Виктория, Никонова Людмила. (2017). Киберпреступность: Международный уровень решения проблемы, - *Электронный сборник статей по материалам XII студенческой международной заочной научно-практической конференции*, Vol. 1, No. 12. Новосибирск: Сибак, 418-423.

Estonian legislation

48. KarS, RT I, 30.12.2017, 29
49. KrMS, RT I, 05.12.2017, 8
50. HasMS, RT I, 25.04.2012, 1 (valid until 05.06.2012)

EU and international legislation:

51. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

Other court decisions:

52. Microsoft cort vs USA. Supreme court of the United States, 17.04.2018, 584 U.S___(2018)
53. United Kingdom Supreme Court decision, 30.01.2018, UKSC 2016/0159
54. USA vs Nikolay Nasenkov and Aleksandr Kalinin casus, sealed indictment S1 09 Cr. 1093
55. Yahoo v Belgium. Hof van Cassatie van België, 1.12.2015, Nr. P.13.2082.N
56. Решение Мещанского Районного Суда г. Москвы, 16.10.2017, 5-1794/2017
57. Решение Таганского Районного Суда г. Москвы, 13.04.2018, 02-1779/2018

Other Sources:

58. 2016 Financial Cybersecurity Report, (2016). SecurityScorecard
59. Alladin Knowledge Systems 2016 report https://www.surf.nl/en/knowledge-base/2016/cyber-threat-assessment-2016.html
60. Alladin Knowledge Systems 2017 report https://www.surf.nl/en/knowledge-base/2017/cyber-threat-assessment-2017.html
61. American Registry for Internet Numbers // Materials of the website of the Internet registrar ARIN. - Access mode: https://www.arin.net/

62. APWG Phishing Attack trend Report Q1 and Q2, 2016
63. BBC Russia, 11 "друзей" Роскомнадзора: какие сайты запретили в России, 12.12.2017 (https://www.bbc.com/russian/news-42324276)
64. Electronic Crime Scene Investigation: A Guide for First Responders. April 2008. US department of Justice, 2nd editon.
65. An integrated vision to manage cyber risk, (2017). EY.
66. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_4-4/regional_internet_registries.html
67. https://ecrimeresearch.org/
68. https://www.actionfraud.police.uk/news
69. https://www.antiphishing.org/resources/apwg-reports/
70. https://www.crunchbase.com/person/gadi-evron/timeline/timeline
71. https://www.radicati.com/?page_id=54
72. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
73. Internet Corporation for Assigned Names and Numbers // Materials of the Internet Registrar's Site.
74. MarkMonitor report available after registration at https://info.markmonitor.com/online-barometer-fraud
75. Official Apple support website https://support.apple.com/en-us/HT204759
76. Regional Internet registrars / / Materials of the site of the company CISCO.
77. See more about 3G and 4G at
78. Symantec report 2017
79. The Guardian, (2017). UK fraud hits record £1.1bn as cybercrime soars.
80. U.S. consumers and cyber-crime – Statistics & Facts 2017
81. Äripäev, (09/10/2012) Uus püramiidskeem huulutab, Available at: https://www.aripaev.ee/uudised/2012/10/09/uus-puramiidskeem-hullutab