Journal of Positive School Psychology http://journalppw.com
2022, Vol. 6, No. 6, 9028-9039

Forms Of Cybercrime And Prevention Of Cybercrime In The Republic Of Northern Macedonia

[1]Muhamet Racaj , [2]Mitasin Beqiri and [3]Senat Saliu

[1]Associate Professor, College "BIZNESI", Republic of Kosovo 10 000 Pristina, Ulpianë Str. "Motrat Qiriazi" No.18 Pristina, Republic of Kosovo, Email: muhamet.racaj@kolegjibiznesi.com
[2] Associate Professor, College "BIZNESI", Republic of Kosovo 10 000 Pristina, Ulpianë Str. "Motrat Qiriazi" No.18 Pristina, Republic of Kosovo, Email: mitasin.beqiri@kolegjibiznesi.com
[3]Assistant Master, AUE – FON University, Str. Kiro Gligorov b.b. 1000 Skopje, Skopje, Republic of North Macedonia, Email: senat.saliu@fon.mk

ABSTRACT

Today's information society faces a number of challenges in the fight against organized crime, especially "cybercrime and cyber-terrorism" as new models of threats in the 21st century. The more sophisticated information technology becomes, the more complex the methods and tools used to combat criminal activity, especially in cyber-terrorism.

This paper examines the forms and forms of cybercrime and their characteristics. Also, as part of the research in this paper, the types of cybercrime that appear in the Republic of Northern Macedonia during the past years are reviewed and an analysis of the forms that occur in our country is performed.

Keywords: cybercrime, criminal offense, prevention, types of cybercrime.

I. INTRUCTION

The world today is in a phase of technological change and innovation, which leads to changes in all parts of modern life and the establishment of the so-called information society. In order for the Republic of Northern Macedonia to be an advanced information society, several issues need to be analyzed. Such an information society faces a number of challenges in the fight against organized crime, especially "cybercrime and cyber-terrorism" as new models of threats in the 21st century. The more sophisticated information technology becomes, the more complex the methods and tools used to combat criminal activity, especially in cyber-terrorism. [1]

The Republic of Northern Macedonia is no exception to the countries that are increasingly facing this sophisticated type of organized crime. The goal of the Republic of Northern Macedonia is to be part of the global security network in the fight against money laundering, organized crime, terrorist financing and the entry of "dirty money" into the economy. Our country needs to make efforts to protect itself from various criminal activities such as theft of personal data, high security secrets, military plans and fraudulent activities such as "stealing money" from credit/debit cards and more. Cyber terrorism and criminal activities have a visible negative impact on the country, namely its economy, the security of its citizens, public life and human rights and freedoms. For all the above reasons, this new form of organized crime should be prevented from further spreading not only in our territory, but throughout the world.

II. THE NOTION OF CYBERCRIME

One of the biggest problems of criminology is giving a definition of new forms of crime. Although there are several definitions, there is no common denominator that is generally accepted.

It is very difficult to form a definition in which all cybercrime crimes can be categorized, due to the great diversity of all forms of such criminal behavior. Cybercrime is just a general form through which various forms of criminal activity are expressed, it is a special type of crime directed against computer systems as a whole, or a part, in different ways and by different means, with the intention of gaining for themselves or someone else some benefit or cause harm to someone else. [2]

In the criminological literature there is an understanding that cybercrime is part of economic crime, but also that it is a crime in the field of property protection and that computer crimes by their nature are closest to crimes in the field of property protection. The most common definition in criminology defines cybercrime as the sum of all types of delinquent behavior by which data processing devices are used as a means of committing criminal offenses or as a direct target for criminal offenses. [3]

The US Department of Justice in the 1979 Handbook of Justice (The Criminal Justice Resource Manual on Computer Crime) gave the first definition of cybercrime, in which cybercrime is any offense whose successful prosecution requires a good knowledge of computer technology.

A working group of UN experts at the XI Congress on Crime Prevention and Criminal Justice held in 2005 in Bangkok, Thailand, defines cybercrime in terms of its prevalence and the danger it poses, as a general term. for crimes committed with the help of a computer system or network, in a computer system or network, or against a computer system or network.

The European Commission in a statement issued in 2001 defined cybercrime in the broadest possible sense, so that cybercrime is any crime that in any way involves the use of information technology. [4]

PhD. Vladimir Vodineliq defines cybercrime in a true (narrower) and incorrect (broader) sense, which in a narrower sense includes computer fraud, sabotage and espionage, and in a broader sense refers to the misuse of computers and its components by theft , embezzlement, etc. [5]

According to PhD Vidoje Spasic Cybercrime is a crime that takes place in the digital environment and is a specific form of illegal action in which the computer network appears as a tool, purpose or evidence to commit a crime. [6]

Given that there are significant definitions that cybercrime is defined by the representation of different views, it is still a general impression that there is no definition that covers all the complexities and problems of cybercrime.

III. CHARACTERISTICS OD CYBERCRIME

Compared to traditional forms of crime, cybercrime is rapidly changing the forms and forms of manifestation, the borders between states and the type of victim. These crimes are hidden, often without a visible and close spatial connection between the perpetrator and the victim. Often difficult to detect, and even more difficult to prove, they remain almost unknown for a long time, until the victim has suffered any damage that is visible in the computer system. [7]

Therefore, an important feature of cybercrime is its phenomenological diversity and great dynamics of development. [8] The number of manifestations of cybercrime is huge and is constantly growing, thanks to the continuous development of technology, with new and more complex forms of cybercrime appearing every day. As computer technology is used in all walks of life, the opportunities for abuse are increasing day by day, with much more dangerous forms of criminal behavior now emerging that were not previously known in criminal and judicial practice.

Another important feature of cybercrime is that it does not know the borders between countries and continents. The spread of Internet use in the world has especially contributed to this feature. The executor can be from anywhere in the world, attacking a particular computer system, no matter where it is, and this is provided primarily by the high speeds of today's computers, so that space and time frame are of little importance in most forms of cybercrime.

Cybercrime is mainly dealt with by people who know information technology very well. In the early years of the development of information technology, great expertise was a prerequisite for operating a computer, which led to difficult detection of crimes. The situation today is changing, the availability and simplicity of computer use and the spread of computer literacy allow the use of computers by a wide range of people, which are an inevitable part of business premises and households, and thus reduce the time required to acquire the necessary knowledge and skills to commit cybercrime.

Because these are distance crimes, the risk of detecting the perpetrator is very small, as well as the fact that this work is performed in an electronic environment, gives this type of crime certain characteristics, namely that these acts are committed faster, easier, in different ways from the point of view of criminals significantly anonymously, because modern information technology provides more than ideal conditions for perpetrators to hide their criminal activities.

It is therefore difficult to gather accurate data on the spread of cybercrime, the structure of crime and its consequences, so the dark figure is huge. According to some estimates, it ranges from 90% to 99%. [9] One of the main problems in preventing and combating cybercrime is the fact that only a small number of crimes are obtained and solved by the police and the judiciary. The dark count of cybercrime is characterized by the following factors: the probability of detection is low, irregularities in communication about the work done; inadequate protection; increase in the number of computers conditioned increase in the number of potential perpetrators, difficult finding of material traces of the committed crime. [10]

IV. FORMS OF CYBERCRIME

Computer theft. The main feature of this form is the illegal seizure of things by others. There are many different and varied forms in which this work appears, as well as the ways in which they are realized. One of the possible ways of classification is according to the subject that is adopted from this part. In this regard, in the field of cybercrime, there are the following typical forms of theft: theft of computers and computer components; data theft; theft of computer services; stealing code passwords and identification numbers. [11]

There are basically two ways to realize this part: the classical form, which means physical entry into the premises and theft of computers and computer equipment and other things that are illegally appropriated, and another way, which means logical intrusion into a computer system and illegal appropriation of computer data, codes, etc.

Computer scams. Computer fraud is the most common form of cybercrime and is found in every part of the business, which can affect the flow of goods and money. Computer fraud is by nature the closest thing to economic crime, and in the literature, almost without exception, these phenomena are treated as the occurrence of economic crime. Computer fraud is most prevalent in the following areas: financial management, insurance, taxes, social security, bankruptcy, and money laundering. [12]

A general feature of this activity is to mislead someone in order to gain illegal property gain. The number of forms of computer fraud, as well as the manner of their realization is practically unlimited, and in practice they are found from very primitive and rude, to those in which the perpetrator has a high degree of skill and refinement.

Computer fraud. Computer fraud means manipulating data in order to gain material gain. Forms of computer fraud are data that are a commodity in information systems. The goods are actually data presented, for example: in the form of money, pledge rights, working hours, credit rating, balance sheet, passwords, codes, identification numbers, etc.

The main feature of this part is to obtain illegal property gain by appropriating the value from the one to whom these values are entrusted. Computers and information technology have been used for embezzlement such as: forgery of accounting documents, fictitious accounts, fictitious travel orders; creating a fictitious payroll, creating fictitious inventory lists, creating fictitious clients, artificially increasing the stock of goods, incorrectly displaying the losses of goods, falsifying credit reports, creating false financial data and in other cases. [13]

Computer forgery. A general feature of this work is the creation of fake or modification of real objects, using a computer, in order to obtain illegal property gain. Typical forms of using information technology for the purpose of forgery are: forgery of documents; forgery of public documents; counterfeiting value marks; forgery of characters for marking goods; counterfeiting money; forgery of a signature; counterfeiting stamps; counterfeiting of securities. [14]

Violation of privacy with the help of information technologies. Information technology enables the storage of vast amounts of data about individuals. The data is collected and stored in electronic databases, which later enable fast processing and retrieval. Developed countries lead in the use and development of technologies for widespread population control and surveillance.

Computer sabotage. Computer sabotage according to the current practice usually consists of damaging or destroying computers or other automatic data processing devices within computer systems, or acting on the perpetrators of information contained in the computer memory, which erases, alters or alters them, prevents their use. Sabotage can act on working or user mechanisms that are primarily in function of data storage. [15] A general feature of this act is covert and insidious acting in the performance of official or work duties, thereby causing harm to others.

There are two basic forms of computer sabotage: logical sabotage and physical sabotage. [16] Physical sabotage means physical damage to computers and computer equipment, logical sabotage means deleting, damaging or changing data, programs or parts of the operating system.

Creation and distribution of harmful programs called malware belongs to computer sabotage for the purpose of destroying or damaging data or computer networks. [17] Malicious programs include viruses, trojans, worms, bombs and droppers, web downloads, and steganography. [18]

Computer espionage. A general feature of this type is the disclosure of secrets, and the basic form consists in passing or making available confidential data using computers and information technology. The intelligence services are engaged through their members to uncover the political, military, economic and official secrets of other countries.

Computer pornography. The subject of protection of this illegal behavior is the dignity of the person and complete freedom. [19] Minors and children are special protection groups, which is why the monitoring bodies pay great attention to the contents on the Internet, which contain explicit sex scenes with children and minors. In essence, this is a crime in the legislation, in which there are four forms: production of child pornography, its sale, dismantling and making available. Due to the fact that pornographic materials seriously hurt morality and that there is constant work of the competent authorities and the fight against their destruction, it is incomprehensible that the market of pornographic materials is constantly expanding. Computer technology has made a key contribution to this. Thanks to the Internet, pornography is available all over the world in various forms, such as pictures, videos, texts, animations, etc.

Computer propaganda. The Internet also serves countries to control the media and form an opinion for the sake of public opinion. Internet propaganda can be used to commit crimes such as: calling for a violent change of the constitutional order; inciting national, religious, racial hatred and intolerance; spreading lies; inciting an aggressive war. Many users through computers connected to various Internet sites and social networks can thus carry out various propaganda activities with a negative sign, spreading ideological, racial, religious, national, hatred through the Internet, which allows terrorist groups to often spread their influence.

Cyber-terrorism. Information technologies are becoming a common tool and target of terrorists. Also, information technology is increasingly emerging as a means of committing the crime of “Terrorism”. The main feature of this act is the perpetration of violence. There are several forms and ways of performing this work. One of the important components of terrorism is the psychological warfare, in which the killing of innocent civilians is a justified measure of intimidation that conveys messages through modern technology available to the masses globally, in order to cause panic and insecurity. and are for the purpose of achieving certain political goals. Thanks to information technology, terrorist groups today are more easily connected and enabled to easily recruit members and spread their ideas. Terrorist organizations also include hackers and other IT professionals who attack the hardware and software resources of certain countries, their organs, and various other economic organizations.

Terrorists use information technology to achieve their goals as follows:

They use the computer as a tool, i.e. through their websites and forums they collect new members, information and funds with which they finance their work by giving statements to the public.

Using computers as archives for its members, financiers, plans, reports, movements of their members, number of bank accounts, list of assistants, etc.

Unauthorized intrusion into the systems of security services and other government agencies, as well as economic and natural persons' subject to their interests. [20]

Hacking. The main feature of hacking is disruption of the protection system and unauthorized access to information systems. The word hacking is derived from the English language and in free translation means man against the computer. [21] There are several forms of realization of this activity. Most often, hackers, using various methods and techniques, obtain all the information necessary for a successful intrusion into someone else's information system, or thanks to predefined programs that are designed to avoid the usual parameters of protection, they enter someone else's information systems. Achieving this goal requires a great deal of knowledge of mathematics and electronics.

Creation and distribution of viruses. This form of cybercrime is inevitable in all criminological divisions. The main feature of the work is the creation and distribution of computer programs - viruses, whose sole purpose is to cause harm to third parties. A computer virus is a program that performs unauthorized actions on a user's system without his knowledge and permission. There are two ways to do this, where the first is the creation of the virus and it is always a conscious action, while the distribution can also be an unconscious action. Computer viruses can make various changes to systems, but the most common are: changes in program size; slowing down programs and systems; incorrect execution of the program; disabling the functioning of the system and disabling it; changes to the program file; destruction of content; copying unnecessary and harmful programs and information; reducing the available free space in the system, etc. [22]

Software piracy. The main feature of the work is the use or duplication of illegally obtained software. Two basic forms of this work are the use of illegal copies and the distribution of such copies. The term software piracy came into use in the 1980s and includes the phenomenon of individuals illegally copying and using or reselling other people's programs. The term is usually used to steal software that was previously intended for sale.

V. LEGAL REGULATIONS IN THE REPUBLIC OF NORTHERN MACEDONIA

The Republic of Northern Macedonia started the fight against terrorism by participating in various seminars and conferences related to the topic of cyber-terrorism. [23] Northern Macedonia has also ratified a number of international conventions related to cybercrime. In 2004, Northern Macedonia ratified the Convention on Cybercrime adopted by the Council of Europe in 2001, as well as additional protocols on criminal acts of a racist and xenophobic nature through computer systems. These international legal acts are in accordance with the domestic legal regulations.

The provisions thus defined are also introduced in the Macedonian substantive legislation, in the part of the general provisions where the basic notions of this type of crime are defined, as well as specific criminal acts. The domestic legal framework governing cybercrime includes:

Criminal Code (CC): [24] Criminal Procedure Code (CPC), [25] Electronic Communications Law, [26] Communications Surveillance Law, [27] Electronic Commerce Law, [28] Electronic Governance Law, [29] Law on Civil Procedure, [30] Law on Electronic Data and Electronic Signature, [31] Declaration on Safer Internet.

Domestic legislation maintains the continental approach and the norms governing this matter and are enshrined in existing laws, while taking into account the protection of fundamental human rights in relation to the right to free expression and freedom of thought and the right to privacy.

Despite the fact that cybercrime is a constantly changing subject and has novelties that cannot be simply defined (new technologies in mobile telephony, the application of special investigative measures, etc.), and especially when it comes to transnational communication, the Convention as a whole is incorporated in our legislation. This enables easier international cooperation, as well as the opportunity to easily adapt the relevant provisions to new forms of this type of crime.

Substantive law: The substantive provisions for criminal offenses in the field of cybercrime are contained in the Criminal Code and refer to: Article 144 - Endangering security, Article 147 - Violation of the secrecy of letters or other consignments, Article 149 - Abuse of personal data, Article 149-a - Prevention of access to public information system, Article 157 - Violation of copyright and related rights , Article 157-a - Violation of the right of the distributor of technically specially protected satellite signal, Article 157-b - Piracy of an audiovisual work, Article 157-c - Piracy of a phonogram, Article 193 - Showing pornographic material to a child, Article 193- a - Production and distribution of child pornography, Article 193-b - Fraud for sexual intercourse or other sexual activity of a minor under 14 years of age, Article 251 - Damage or unauthorized entry into a computer system, Article 251-a - Making and entering computer viruses, Article 251-b - Computer fraud, Article 271 - Making, obtaining or alienating means of counterfeiting, Article 274-b - Making and using a fake payment card, Article 279-a - Computer forgery, Article 286 - Violation of the right from a reported or protected invention and topography of integrated circuits, Article 394-d - Dissemination of racist and xenophobic material through a computer system, Article 122 - Defining basic segments of cybercrime:

- Item 15 payment cards - Payment cards means any type of payment means issued by banking or other financial institutions that contain electronic data of persons and electronically generated numbers that enable the performance of any type of financial transaction;
- Item 24 Child Pornography - Child pornography means pornographic material which visually depicts obvious sexual acts with a minor or an adult who looks like a minor, or portrays a minor or an adult who looks like a minor in an obvious sexual position or sexual acts with a minor or depicting a minor or an adult who looks like a minor in an obvious sexual position;
- Item 26 computer system - By computer system we mean any device or group of interconnected devices, one or more of which performs automatic data processing according to a specific program;
- Item 27 computer data - Computer data means the presentation of facts, information or concepts in a form suitable for processing through a computer system, including a program eligible to operate the computer system.

Procedural Law: Criminal Procedure Code - The process addresses issues related to cybercrime, with the main emphasis on measures and actions that apply specifically to this type of crime, as well as measures and actions that apply to conventional crime. This includes the provisions of the LCP for search of computer system and computer data (Article 184) and temporary seizure of computer data (Article 198), as well as the provisions of Chapter XVII - Measures for finding and securing persons and objects, further purpose and types of special investigative measures (Article 252), especially the special measures of secret inspection and search in a computer system and inspection of realized telephone and other electronic communications, etc. [32]

Cybercrime, like conventional crime, presupposes the collection of evidence which, despite their physical presence, requires the collection of data that are not visible [33] and is in a form that presupposes their previous detection and fixation through physical form (computer, workstation, telephone and etc.) and then undertaking additional procedural actions that presuppose indirect contact with evidence in electronic form and places where they are stored.

When gathering evidence, the following are of particular importance: a certificate for temporary seizure of items; which items can be confiscated; ways of temporary confiscation of items; conditions and principles of preserving the authenticity of confiscated items.

In exclusive cases, the gathering of evidence shall be carried out remotely by applying the provisions of Article 32b of the Convention on Cybercrime.

In situations where it is necessary to inspect computers that are currently running, it is extremely important that there is no power outage, as RAM stores data as long as there is power, otherwise it may be lost.

VI. CYBERCRIME AUTHORITIES IN THE REPUBLIC OF NORTHERN MACEDONIA

The beginnings of the Sector for Cybercrime and Digital Forensics (SCDF) are in February 2005 when the Department for Cybercrime and Counterfeiting was established for the first time, within the Sector for Financial Crime at the Department for Organized Crime. In October 2008, the Unit grew into a Unit for Combating Cybercrime within the Department for Combating Organized and Serious Crime. In November 2014, the Unit separated from the Department of Organized Crime and grew into the Sector for Cybercrime and Digital Forensics within the Central Police Services. Thereby, the Sector has competence to act on the entire territory of the Republic of Northern Macedonia.

SCDF is composed of two departments:

Computer Crime Investigation Unit, which has two departments: The Payment Card Abuse Investigation Division and the Computer Incident Investigation Division.

- The unit primarily acts on criminal acts in the field of computer crime which are provided in the Criminal Code of RNM, as follows:
- Acts on criminal acts in the field of Damage and unauthorized entry into a computer system (Article 251 and Article 251a)
- Acts on criminal acts in the field of sexual abuse of minors or children (Article 193, Article 193-a, Article 193-b)
- Acts on criminal acts in the field of internet fraud (Article 247)
- Acts on criminal acts in the field of personal data (Article 149)
- Acts on criminal acts in the field of misuse of payment cards (Article 271, Article 274-b).

Digital Forensics Department, which has two departments: Computer Equipment Examination Department and Mobile Devices Examination Department.

The Department, with a prior order issued by a Court or Public Prosecutor, analyzes the submitted computer equipment and telephone devices and prepares a finding and opinion in accordance with Article 236 and Article 222 of the Law on Criminal Procedure. The department is responsible for all cases of analysis of computer equipment and mobile devices on the territory of the Republic of Northern Macedonia. The Cybercrime and Digital Forensics Department cooperates with both Interpol and Europol.

There are no special specialized institutions in the Republic of Northern Macedonia that deal with cyber terrorism and that legally investigate it. This is because in Northern Macedonia cyber terrorism is not legally defined, regulated and accepted. However, there are state institutions responsible for certain aspects of cyber terrorism, such as information technology protection and security in general. These institutions consist of: The Ministry of Information Society, the Public Security Bureau, which is part of the Ministry of Interior, the Ministry of Defense, the Crisis Management Center and the Agency for Electronic Communications. These institutions agreed to coordinate activities and define the institutional basis for norm-building and intensive international cooperation in the fight against cyber terrorism.

VII. OVERVIEW OF CYBERCRIME RELATED IN THE REPUBLIC OF NORTHERN MACEDONIA

Table 1 provides an overview of criminal acts that enter into cybercrime in the territory of the Republic of Northern Macedonia.

Table 1. Overview of criminal offenses entering cybercrime for the period 2015-2020

Criminal offense	**2015**	**Perpetrators**	**2016**	**Perpetrators**	**2017**	**Perpetrators**	**2018**	**Perpetrators**	**2019**	**Perpetrators**	**2020**	**Perpetrators**
Damage and unauthorized entry into a computer system Article 251	40	33	70	40	43	34	53		65		85	
Computer fraud Article 251 b	8	3	12	3	13	12	14		12			
Issuance of a check without cover and misuse of a payment card Article.274												
Making and using a fake payment card Article 274 b	9	6	13	25	12	14			8		18	8

Computer forgery Article 379a												
Total	57	42	95	68	68	60	67		85		103	8

Source: Ministry of Interior (Annual Report of the Ministry of Interior)

In the period 2015-2020 on the territory of the Republic of Northern Macedonia are not registered criminal acts “making and importing computer viruses” Article 251-a of the Criminal Code, while in the period 2015 - 2020 are registered other forms of computer crime which are given in Table 2.

Table 2. Overview of other crimes for the period 2015-2020

Criminal offense	**2015**	**Perpetrators**	**2016**	**Perpetrators**	**2017**	**Perpetrators**	**2018**	**Perpetrators**	**2019**	**Perpetrators**	**2020**	**Perpetrators**
Endangering security Article 144/4	3	2	3	1	5	2	21		29		28	25
Abuse of personal data Article 149/2			1	1	1	1			19			
Violation of the right of the distributor to technically specially protected satellite transmission Article 157a	1	1										
Showing pornographic material to a child Article 193	3	3	8	5					4	2	4	2

Production and distribution of child pornography Article 193 a	7	7	7	5	4	6			6	5	2	
Cheating on an adulterer or other sexual act of a child under 14 years of age Article 193 b					2	2					2	2
Making, obtaining or alienating funds for counterfeiting Article 271/3			2	2	1	1						

Source: Ministry of Interior (Annual Report of the Ministry of Interior)

VIII. CONCLUSION

The Republic of Northern Macedonia is no exception to the countries that are increasingly facing cybercrime. The goal of the Republic of Northern Macedonia is to be part of the global security network in the fight against money laundering, organized crime, terrorist financing and the entry of "dirty money" into the economy. Our country should make efforts to protect itself from various criminal activities such as theft of personal data, high security secrets, military plans and fraudulent activities, "stealing money" from credit/debit cards. Cyber-terrorism and criminal activities have a visible adverse effect on the country, i.e. its economy, the security of its citizens, public life and human rights and freedoms.

Cybercrime is just a general form through which various forms of criminal activity are expressed, it is a special type of crime directed against computer systems as a whole, or a part, in different ways and by different means, with the intention of gaining for themselves or someone else some benefit or cause harm to someone else.

Compared to traditional forms of crime, cybercrime is rapidly changing the forms and forms of manifestation, the borders between states and the type of victim.

Computers and information technology can serve to commit traditional forms of crime, but also completely new forms of abuse of computers, computer systems and crime-related networks. Traditional forms of crime include computer theft, embezzlement and fraud, forgery. New forms of cybercrime include specific crimes that can only be committed using computers, computer systems, and networks. These are, for example, hacking, creating and distributing viruses.

The use of scientifically derived and proven methods of preserving, collecting, validating, identifying, analyzing, interpreting, documenting and presenting digital evidence obtained from digital sources in order to facilitate or prolong the reconstruction of criminal events, or to help anticipate unauthorized acts have proved to be unacceptable for planned operations represent digital forensics operations.

References

[1]http://eprints.ugd.edu.mk/10870/1/Skripta%20za%20Sigurnost%20na%20kompjuterski%20sistemi%2Ckompjuterski%20kriminal%20i%20terorizam_revJA_2.pdf

[2] Parker, B.D., Fighting computer crime, New York (USA), 1983, pp.70.

[3] Konstantinović-Vilić, S., Nikolić-Ristanović, V., Kriminologija, Niš, 2003, pp.178-179

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2001:0051:FIN

[5] Šarkić, N., Prlja, D., Damnjanović, K., Marić, V., Ţivković, V., Vodinelić, V., Mrvić-Petrović, N.: Information Law, Belgrade, 2011, pp.3.

[6] Spasić, V., Current issues in the field of cybercrime (article), Bulletin of judicial practice of the Supreme Court of the Republic of Serbia, no. 1/2006, Belgrade, pp. 107.

[7] Zivkovski, Z. I., Detection and clarification of computer crime; Article, 2012, pp. 162-165.

[8] Gillespie, A. A., Cybercrime: Key Issues and Debates Florence, Kentucky (USA), 2015, pp.17.

[9] Dimovski, D., - Computer crime, Niš, 2010, pp.205.

[10] Feješ, I., Computer crime – the crime of the future, the challenge of the present – conference presentation, 2000, pp. 378.

[11] Petrović, R S., Computer crime; Ministry of Internal Affairs of the Republic of Serbia: Editorial Board of the magazine “Bezbednost” and the newspaper “Policajac”, /Belgrade 2000, pp. 117.

[12] Matijašević, J., Criminal law regulation of computer crime; Faculty of Law for Economy and Justice, Novi Sad, 2013 pp. 166.

[13] Petrović R. S.; Computer crime; Ministry of Internal Affairs of the Republic of Serbia: Editorial Board of the magazine “Bezbednost” and the newspaper “Policajac”, Belgrade 2000, pp. 131.

[14] Toren, J. P., Intellectual Property and Computer Crimes (Intellectual Property usiness Crimes Series), New York USA, 2003, pp. 6-41

[15] Cvetković, Z., Computer crime – article, 2011; pp. 7-8.

[16] http://www.nytimes.com/2010/09/30/world/middleeast/30worm.html?_r=0

[17] http://techterms.com/definition/malware

[18] http://www.kaspersky.com/internet-security-center/threats/malware-classifications

[19] ĐurĊić, V., Jovašević, D., Criminal law: special part, Niš, 2013, pp.79.

[20] Campbell E. D., Computer Terrorism, Syneca Research Group, Inc. Washington USA, 2011.godine, pp.13-17.

[21] http://en.wikipedia.org/wiki/Hacker_%28computer_security%29

[22] Petrović R. S., Computer crime; Ministry of Internal Affairs of the Republic of Serbia: Editorial Board of the magazine “Bezbednost” and the newspaper “Policajac”, Belgrade 2000, pp. 185.

[23] Activities for prevention and dealing with the consequences of cyber terrorism. Ministry of Information Society http://www.mio.gov.mk/?q=node/1911

[24] Official Gazette of RM, No.37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 50/2006, 60/2006, 73/2006, 87/2007, 7/2008, 139/2008, 114/2009, 51/2011, 51/2011,

135/2011, 185/2011, 142/2012, 143/2012, 166/2012, 55/2013, 82/2013

[25] Official Gazette of RM, No.150/2010, 100/2012

[26] Official Gazette of RM, No.13/2005, 14/2007, 55/2007, 98/2008, 83/2010, 13/2012, 59/2012, 123/2012, 23/2013.

[27] Official Gazette of RM, No.121/2006, 110/2008, 4/2009, 116/2012

[28] Official Gazette of RM, No.133/2007, 17/2011

[29] Official Gazette of RM, No.105/2009, 47/2011

[30] Official Gazette of RM, No. 79/2005, 110/2008, 83/2009, 116/2010

[31] Official Gazette of RM, No.34/2001, 98/2008

[32] Zvrlevski., M., Handbook of computer crime, Skopje, 2014

[33] CASX – data found in the active memory of a computer