UDK: 343.9.02::004
Biblid 0543-3657, 63 (2012)
Vol. LXIII, No. 1147, pp. 5–21
Original Scientific Paper
October 2012

Željko Bjelajac,
Jelena Matijašević,
Duško Dimitrijević[1]

Computer Fraud as a Part of Contemporary Security Challenges

ABSTRACT

In the present conditions of life, there is no area of human activity in which computers have found their application. Computer frauds are, by nature, certainly the nearest commercial crime, and make it illegal to obtain economic benefits. Computer fraud in the Criminal Code of the Republic of Serbia is prescribed as an individual criminal act and is covered by Article 301 Criminal Code. Surveys based on the data of the Special Prosecutor for cyber crime established in the Higher Public Prosecutor's Office in Belgrade, and the period in 2008, 2009 and 2010, it was found that the offense of computer fraud in the present practice of the judicial authorities of the Republic of Serbia. Based on the analysis of the number of criminal charges by year, there is an evident increase in detection of computer fraud offenses compared to other crimes in the area of cyber crime.

Keywords: computer fraud, cyber crime, economic development, budget policy.

[1] Prof. Dr. Željko Bjelajac, Faculty of Law for Business and Justice in Novi Sad, E-mail: zdjbjelajac@gmail.com.

Doc. Jelena Matijašević, Faculty of Law for Business and Justice in Novi Sad, E-mail: jelena@pravni-fakultet.info.

Dr. Duško Dimitrijević, Institute of International Politics and Economics, Belgrade, E-mail: dimitrijevicd@diplomacy.bg.ac.rs. The paper is the result of the Project of the Ministry of Education and Science, within the Programme for basic research for the period 2011–2014, entitled "Serbia in Contemporary International Relations: Strategic Directions for the Development and Strengthening the Position of Serbia in the International Integration Processes – Foreign Policy, International Economic, Legal and Security Aspects."

Introduction

We are all aware of the enormous importance of the use of computers in contemporary society and the fact that there is no area of human activity in which computers have found their application. Thanks to a huge computer power saving and fast in processing large amount of data, automated information systems are becoming increasingly numerous and almost indispensable part of the entire social life of all subjects (physical as well as legal persons) at all levels. However, it is a pretty devastating conclusion that there is no technical and technological achievement in the history of mankind has not been met with various forms of abuse. The specificity of a phase of development in which the invention has been subject to abuse, then the group of persons who committed such acts and different purposes for which they are inflicting this abuse.

At the beginning of computer technology, computers were not suitable for the increasing abuse, given that their application was not massive so that they handled only a narrow range of users — IT professionals. What opened the door to expanding opportunities to misuse computer technology in various applications is its rapid development, simplifying its use, as well as the availability of the same wide range of users.

One of the most important forms of cyber crime includes computer fraud.

Criminological framework of computer fraud

Computer frauds are inherently the closest to an economic crime, and in the literature, almost without exception, these phenomena are treated as a manifestation of economic crime.[2]

Computer frauds are the most common form of computer crime, which often cause enormous harm to. Computer fraud is carried out in order to obtain for himself or for another unlawful gain, with such things as they do not lead into fallacy or keep a person, as in the case of ordinary fraud in property crimes, but that fallacy relates to a computer in which incorrect information are entered or fail to enter the correct data, or in any other way the computer is used for the realization of fraud in the criminal sense.[3]

---

[2] Božidar Banović, *Preservation of evidence in crime-processing crime economic crime*, Police College, Belgrade – Zemun, 2002, p. 140.

[3] Živojin Aleksić i Milan Škulić, *Crime*, Faculty of Law, University of Belgrade and Služeni glasnik, Belgrade, 2007, p. 389.

Most numerous computer frauds are, in fact, in the area of financial management, insurance, taxes, social security, in connection with the declaration of bankruptcy, money laundering, and so on.

Computer fraud is defined in 1989 in a document of the Council of Europe as an input, alteration, deletion or suppression of computer data or programs, or otherwise interfering with the process of data processing that causes damage to another person or property, with the intent to obtain an unlawful economic gain for himself or another person.[4]

Computer fraud can be performed in a wide variety of ways, and computer-offenders in this regard a really showing great ingenuity.[5]

In foreign practice, there were cases of many years of paying child benefit to people who do not have children, remittances fictitious companies that were established for this and that and then immediately shut down, the payment of pensions and benefits for an accident to employees for healthy people. In banks, the typical method of execution is to round up the sum on the accounts of customers to integers, so the difference was electronically routed to their own account. Similar transactions are possible when there is a change in interest rates for the benefit of depositors, or changes in exchange rates, and this fact is not recorded in a while, and so on. That's one officer in Hamburg Savings Bank issued an order to the computer, the calculation of interest, and dozens of rounds hundredths pfennig and remains the number rounded up, it automatically transfers to his account in the same bank. In this way, in just two years, she's unlawful gain of about 500,000 German marks.[6]

Computer fraudsters abusing the very features of cyberspace that contribute to the growth of electronic commerce: the anonymity, the distance between seller and buyer, and the current nature of the transaction. In addition, they are taking advantage of the fact that fraud on the Internet does not require access to a payment system, as required by any other type of fraud, and the digital market is still under-regulated and as such is confusing for consumers, which for them is almost ideal conditions for fraud.[7]

---

[4] Council of Europe, Recommendation No. R (89) 9 of the Committee of Ministers to member states on Computer-related crime,https://wcd.coe.int/com.instranet.InstraServlet?command =com.instranet. CmdBlob Get&InstranetImage=610660&SecMode=1&DocId=702280& Usage=2.

[5] See more: Bellour J. C.: "The International", *Choice No.1,* 1981, p. 76–77, quoted in: Aleksić i Milan Škulić, *Criminalistics*, op. cit., p. 389.

[6] Heidel Wolfgang: "Taglich 500 Milliarden USD – Transaktionen uber EDV", *Kriminalistik*, 12/1984, p. 589; quoted in: Božidar Banović, *Preservation of evidence in crime-processing crime economic crime*, op. cit., p. 141.

[7] Cybercrime, Security Consulting APIS; http://www.apisgroup.org/sec.html/Knjige/UMOB /sec.html?id=29 (downloaded: 05.09.2010.)

One of the most spectacular cases of computer fraud Rifkin was the case, which occurred in 1978 in the United States. As an analyst employed by one of the insurance business partners Pacific Bank of Los Angeles, Rifkin had four times the opportunity to enter the room where it is carried out electronically transfer money and unnoticed observe the code that was used for this type of banking operations. He then ordered the transfer of 10.2 million dollars in its account, which was opened at a bank in New York. From this account it was transferred $ 8 million to the account of a Russian merchant in Switzerland, from whom he bought the diamonds out of 9000 cards. For eight days it took the bank to find out what happened, and Rifkin was discovered when he returned to the U.S. and carelessly offered to sell the diamonds purchased.[8]

Weight of computer fraud is even more far reaching as those due to the size of the Internet, then, is very difficult to detect and prove, and because of the low salience, very often these acts are performed for a long time and continuously.

The prevalence, severity and risk of cyber crime sufficiently indicates the fact that in Germany inm 1992 12,435 cases were registered this manifestation of the crime of which makes the 2485 Computer Fraud cases.[9]

The FBI has estimated in 1998 when the price of the scams on the Internet was $ 15 billion. A study made by the FBI, based on a survey of 4200 companies, found that frauds on the Internet has doubled since 1996 to 2000. For on-line sales are fake passports, social security numbers, birth certificates certificate, driver's license, college diploma, journalism credentials and even identification cards for police officers and FBI agents.[10]

According to research Internet Crime Complaint Center (IC3), in the United States, the losses are expressed in fraud in 2006 amounted to 198 million dollars. In 2007, the losses reached the figure of 239 million, where the computer was the means or the object of the attack, while in 2008. the loss in the U.S. increased to 264 million dollars just to Fraud.[11]

The case of a spectacular computer fraud, which the victim was a large London-based bank is also interesting because it revealed an atypical work,

---

[8] Information Corner, Interesting; http://kompjuterskikriminalitet.blogspot.com/2009/02/zanimljivosti.html (downloaded: 15.09.2010.)

[9] Insurance, Journal of Insurance and Business, Zagreb, 1–2/94, p. 47 Quoted by: Šime Pavlović: "Computer crimes in the Criminal Code — the basics of the Croatian Information", *Croatian Annual of Criminal Law and Practice*, Vol. 10, no. 2/2003, p. 625–664, Zagreb, p. 627

[10] Božidar Banović: *Providing evidence in criminal investigations related in economic crime*, op.cit., p. 142.

[11] The Latest Cybercrime Statistics On The Internet, Tech Watch,http://www.techwatch.co.uk/2008/04/04/the-latest-cybercrime-statistics/ (downloaded: 12.02.2011.)

despite the obvious evidence, not prosecuted. Although the offender is managed by skilful operations illegal proceeds to acquire high gain and, thus, thanks to the great attention of the mass media, awakened hopes and fantasies of many people, eager to get rich quick stock adventures. In fact, the developer is like a bank clerk managed to "break" a computer code, and unauthorized use of its transfer into his own account in a Swiss bank account the sum of four million pounds. It appears, however, to the dismay of those responsible in the bank, after a few months of flight from the country, contacted his former employers, to explain to them that the news of stock investing money that was stolen, he managed to realize additional revenue of two million pounds. Insolent offender then sent to the bankers and their "reasonable business proposition" and said he was ready to give them back those initially fraudulently appropriated four million pounds, on condition that the bank commits that it will not prosecute him, and of course the ability to freely retain two million pounds earned in stock business. Choosing between quite certain financial reparations, potential financial damages and completely uncertain criminal prosecution, of course, the bank accepted the proposal offered.[12]

The existing forms of computer crime have emerged in Serbia long before the first criminal legislation in this area. For many years, crime in the areas of computer crime did not have the qualification to them by nature and type of work belonged. It is interesting to mention the case studies of the police, who, on the one hand illustrate some of the forms mentioned spheres that were discovered in the country, and on the other by the way they are legally qualified in the absence of special criminal law, which includes this problems.

The first example is the commission of the crime of computer fraud, which is qualified as a crime of fraud:

Treasurer in a Belgrade bank branches was trained to work on terminals that are used for direct introduction of a new state in the central memory of a computer. Although most of the employees were trained to operate the terminal, it were only the liquidators, who were issued with special keys to start, without which the terminal is not able to handle. These keys, when in contact with the terminal, leaving a trace in the form of codes, in order to know who authorized the liquidators worked at the terminal. However, the relationships among employees in the branch there was the great confidence and is a certified cashier, at the beginning of time were putting the key in the ignition terminal and left it there during the entire working hours. In the course of time, changes in the terminal and enter the other workers, except for the authorized liquidator. The

[12] Milan Škulić, „Cybercrime — how to respond to the challenge, "Proceedings of the Conference on Computer Sciences and Information Technologies YU INFO '98, program areas: Legal Aspects of Computer Science, p. 1225–1230, Kopaonik, 1998, p. 1227.

aforementioned cashier seized the opportunity to lobby and put his savings booklet (which is addressed to the bearer), and demanded payment of 180,000 dinars, although the stakes in the booklet was 2,000 dinars. The computer was programmed so that he could not express his overdraft, but export marked the required amount of payment, and in the "Sheet", again showed the amount of 2,000 dinars. Then he gave the order to reverse payments, register the amount of 180,000 dinars in red letters in the booklet, which is reduced to zero change. The computer had this operations cancellations accepted as payment and payment in the "state" expressed the amount of 180,000 dinars. For treasurer that was signal that is in the memory of computers created a false condition, and was subsequently ordered to pay the whole amount thus obtained self gain.[13]

The existing forms of computer crime have emerged in Serbia following example illustrates a different way of execution, which was qualified as a crime of misconduct:

Clerk in a Belgrade bank over a longer period of time, using the fact that she works in a bank and trust of his colleagues, he took large amounts of checks in other banks raise cash checks issued in the name. He then raised the cash portion paid to your checking account, that one could not be expressed overdrafts, and when they arrived at the realization of the checks, she did not immediately computer-processed, as was her usual job duties, and thus made substantial gain.[14]

Bearing in mind that digital technology when it comes to economic activity, first introduced in banks and other financial institutions, it is only it was there first time misused, which is proved by the previous two examples.

According to research Australian Institute of Criminology (Australian Institute of Criminology)[15] which were conducted over a period of four years (2003 to 2006), in cooperation with the agency AusCERT, the Australian Centre for Cybercrime (Australian High Tech Crime Centre) and several state police agencies, led to the following results: The most frequent manifestation in the field of computer crime is the use of a harmful content, primarily viruses, worms and Trojan horses. After this form, the most represented of computer fraud, particularly fraud of a financial nature, and so internal (insider) abuses of

---

[13] Case study of the Criminal Police, the Secretariat of Internal Affairs in Belgrade; cited by: Božidar Banović, *Preservation of evidence in crime-processing crime economic crime*, op. cit., p. 147–148.

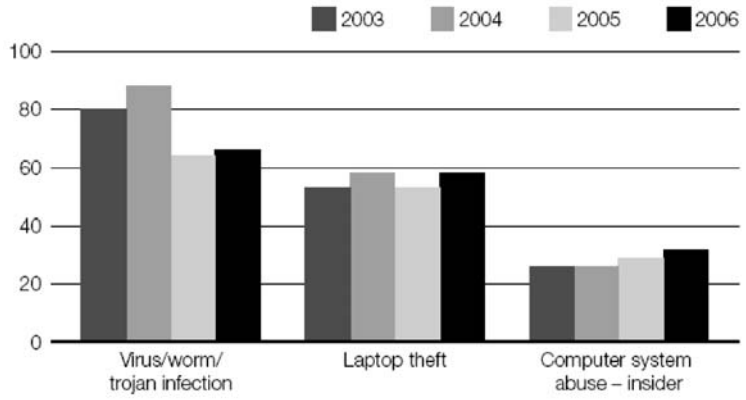
[14] Case study of the Criminal Police, the Secretariat of Internal Affairs in Belgrade; cited by: Božidar Banović, *Preservation of evidence in crime-processing crime economic crime,* op. cit., p. 148.

[15] *Statistics, Fraud and deception-related crimes, Cybercrime*, Australian Institute of Criminology, 2007, Canberra, http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (downloaded: 12.02.2011.)

a computer system. The study covered 181 state institutions and organizations. The amount of damage were worth millions.

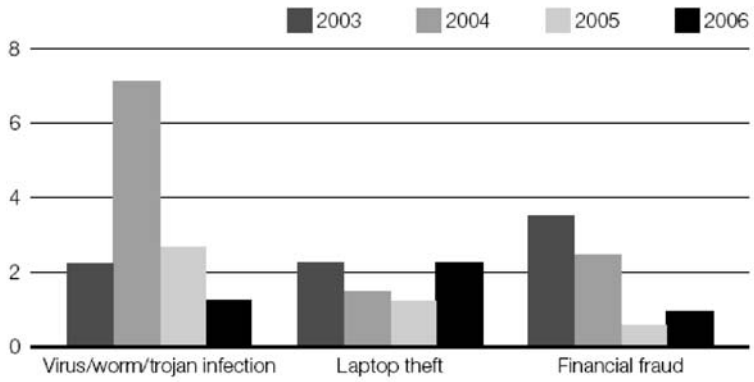
Graphical representation of the type and volume of distribution of these forms of computer fraud, are shown below:

Chart 1: The most common forms of computer crime and security flaws in the period 2003–06 (in percent)



Извор: Australian Institute of Criminology 2007, Australian crime: facts and figures 2006, Canberra, http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (Downloaded: 12.02.2011.)

Chart 2: The main sources of financial losses due to computer crime and security vulnerabilities, 2003–06 (in millions of $)



Source: Australian Institute of Criminology 2007, Australian crime: facts and figures 2006, Canberra, http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (Downloaded: 12.02.2011.)

The criminal justice framework of computer fraud in the Republic of Serbia

The fact that information and communication technologies have become indispensable to the functioning of modern societies, created the need to establish a world scale measures and mechanisms for the protection of society and the individual against abuses in this area, adopting appropriate legislative solutions, and promoting international cooperation. The result of such efforts, among other things, is adoption of the Council of Europe Convention on Cybercrime which established minimum standards that are necessary, in the opinion of the international community to fulfill the national legislation in order to effectively combat cyber crime.[16]

The Republic of Serbia has ratified the said Convention and the Criminal Code[17] included offenses against the security of computer data, which are provided for in Title XXVII of the Criminal Code (Articles 298–304a). The crime of computer fraud is prescribed in Article 301 Criminal Code.

Offense has the basic form, two serious and one particular form. The basic form of the work makes a person who enters false information, fails to enter the correct information or otherwise conceal or misrepresent the data and thus affect the result of electronic processing and transmission of data in order to obtain for himself or other unlawful material gain for the second time and causes property damage. The offense is over when the act of taken with the intent to obtain for himself or for another, an economic benefit or to cause another kind of property damage. For the main part of the prescribed form of a fine or imprisonment of up to three years. There are two forms of serious offenses, depending on the amount of proceeds of the illegal gain. First there is a more severe form when the material gain in the amount of 450,000 dinars, and for him a prison sentence of one to eight years. Other more severe when there is a material gain exceeding one million five hundred thousand, and it is punishable by two to ten years. Special, privileged form a part of the action when the execution takes only the intent to harm another person. For this form is punishable by a fine or imprisonment of up to six months.

The intention of the legislator was prescribing the offense Computer Fraud Protection to credibility and integrity of data being electronically processed or transmitted electronically. It is necessary to determine in each case the intention of the perpetrator, which consists in the fact that for themselves or another to obtain an economic benefit and thereby cause other damage to property.[18]

---

[16] Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001; European Treaty Series (ETS) – No. 185; http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc (Downloaded: 05.08.2010.)

[17] Criminal Code, Službeni Glasnik, No. 85/2005, 88/2005, 107/2005, 72/2009 and 111/09.

[18] Lidija Nikolić Komlen; Radoje Gvozdenović, Saša Radulović, Aleksandar Milosavljević, Ranko Jerković; Vladan Živković; Saša Živanović, Mario Reljanović, Ivan Aleksić, *Combating cyber*

Since the action of the offense defined alternatively as entering incorrect data or failure to enter the correct data, or any other such concealment or misrepresentation of data, the work is finished when undertaken by an act of commission, described the existence of intent and, when another property damage caused as a result, while it is not necessary to be a result of the action taken and realized an economic benefit. This offense can be committed by any person who takes the act of committing premeditated.

In recent years, electronic commerce becomes the dominant way of doing business, and businesses in our state. Segment transactions carried out electronically opens up many possibilities for abuse that may be affected by all economic actors, in case the integrity and validity of the data in their electronic processing are not properly protected.

In previous domestic case law, there were several cases of prosecuting perpetrators of this crime, and the above examples show that computer fraud is becoming increasingly common crime. Thus, the Office of the fight against cyber crime investigation launched against suspect T. A. suspicion was in 2007 and 2008. The two times using computer systems went into banks in Australia and Switzerland, and issued false orders for the transfer of funds, which is obtained by unlawful property gain in the amount of 51,990 CHF, or that he tried to from a Swiss Bank without authorization to transfer funds in the amount of $ 19,000.[19]

Since in our country there are a large number of sports betting with a wide network of branches and whose business is inconceivable without computer networks, often occurring misuse of such systems. Executives in different ways trying to influence the outcome of electronic data processing and using gives software solutions, forge played tickets. Against-M. D. an investigation was launched based on the suspicion that on 22 June 2008. in the premises sportsbook located in Cacak, having born. "Les Folies LLC" as a person employed in the business of receiving and collection of sports tickets, in order to give yourself and another person unlawful material benefit, when entering data into the computer — changed the time on the computer, and pay per ticket for sports betting serial numbers F1 ... F16 ... and, entering, instead of real time, the time when the outcome of matches per paid Ticket holder already known, which is influenced by the result of electronic data processing in the form of monetary gain by registering paid

---

crime, the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, Belgrade, 2010, p. 101.

19 Lidija Nikolić Komlen; Radoje Gvozdenović, Saša Radulović, Aleksandar Milosavljević, Ranko Jerković; Vladan Živković; Saša Živanović, Mario Reljanović, Ivan Aleksić, *Combating cyber crime*, the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, Belgrade, 2010, p. 102.

TIKETA these serial numbers – which is N. N. face, on the following as we as the next day, the amount paid in unlawful material gain of 120,438 dinars.[20]

The prosecution in 2008 opened an investigation against one of the employees of the company "Telecom" reasonable suspicion that in the period since 2003 by 2007 costing the company more than ten million, so falsely portrayed as data related to traffic and tariffing and eighteen telephone connections allow free calls to local, long distance and international calls, as well as all mobile phone networks.[21]

Research in the area of representation of the crime of computer fraud in the practice of the Special Prosecutor for the high-tech crime in the Republic of Serbia

In this section of work, will be shown the practice of the Special Prosecutor for cyber crime established in the Higher Public Prosecutor's Office in Belgrade, in terms of the number of received criminal charges for offenses in the sphere of cyber crime.[22] The period in which they were performed research obtained in 2008, 2009 and 2010. The aim of the research is to determine the number of criminal charges for computer fraud offense for each year covered by the survey, and based on these data ranks share this offense in relation to other crimes in the area of cyber crime. The results follow below.

Special Prosecutor for cyber crime in 2008 were filed 110 criminal charges against 179 persons.[23]

In Table 1 shows the number of persons in 2008 year and filing of criminal charges of crimes cyber crime.

Data from Table 1 are presented in Figure 3 as shown below.

---

[20] Lidija Nikolić Komlen; Radoje Gvozdenović, Saša Radulović, Aleksandar Milosavljević, Ranko Jerković; Vladan Živković; Saša Živanović, Mario Reljanović, Ivan Aleksić, *Combating cyber crime*, the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, Belgrade, 2010. pp. 102–103.

[21] Serious Fraud six million, "Victory"; http://www.pobjeda.co.me/citanje.php? datum=2005-11-19&id=75425 (downloaded: 07.05.2009.); Quoted from: Lidija Nikolic-Komlen; Radoje Gvozdenovic, Sasa Radulovic, Aleksandar Milosavljevic, Ranko Jerković; Vladan Zivkovic; Sasa Zivanovic, Mario Reljanović, Ivan Aleksic: "Combating cyber crime", op. cit., p. 103.

[22] The research based on the original data of the Special Prosecutor for cyber crime established in the Higher Public Prosecutor's Office in Belgrade. More on the Special Prosecutor's Office for cyber crime: http://www.beograd.vtk.jt.rs/ (downloaded: 05.09.2010.).

[23] Data obtained in the framework of the Report of the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in the year 2008.

Table 1: Number of persons against whom criminal charges have been filed for cybercrime offenses — 2008

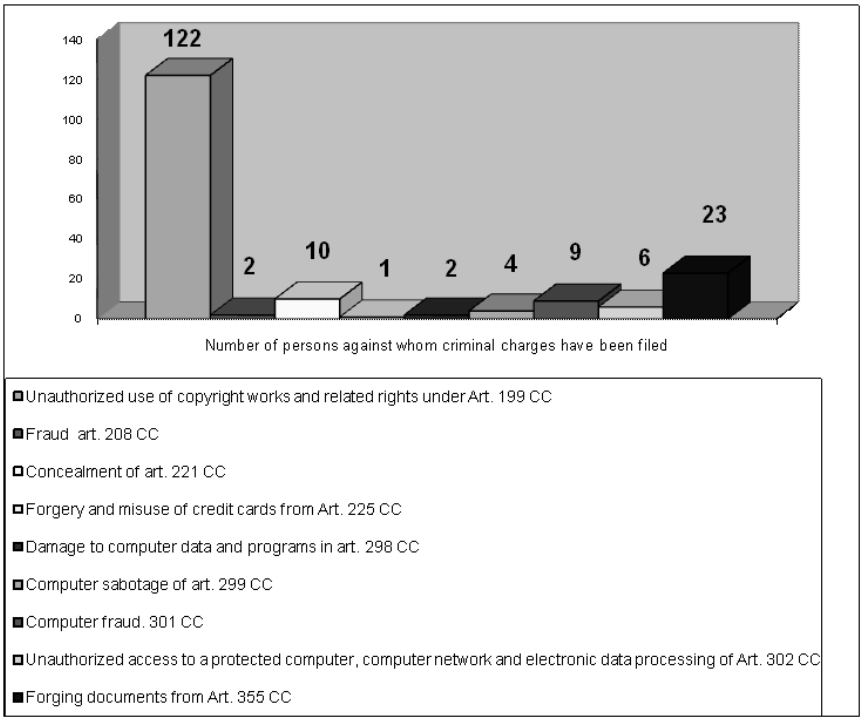
No.	The cybercrime offenses:	Number of persons against whom criminal charges have been filed:
1	Unauthorized use of copyright works and related rights under Art. 199 CC	122 persons
2	The fraud in the art. 208 CC	2 persons
3	Concealment of art. 221 CC	10 persons
4	Forgery and misuse of credit cards from Art. 225 CC	1 persons
5	Damage to computer data and programs in art. 298 CC	2 person
6	Computer sabotage of art. 299 CC	4 persons
7	Computer fraud. 301 CC	9 persons
8	Unauthorized access to a protected computer, computer network and electronic data processing of Art. 302 CC	6 persons
9	Forging documents from Art. 355 CC	23 persons

Source: Data from the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in 2008.

Special Prosecutor for cyber crime in 2009 were filed 91 criminal charges against 113 persons.[24]

[24] Data obtained in the framework of the Report of the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in 2009.

Chart 3: Number of persons against whom criminal charges have been filed for cybercrime offenses — 2008



In Table 2, its showed the number of persons in 2009 year and filing of criminal charges of cyber crime crimes.

Table 2: Number of persons against whom criminal charges have been filed for cybercrime offenses — 2009

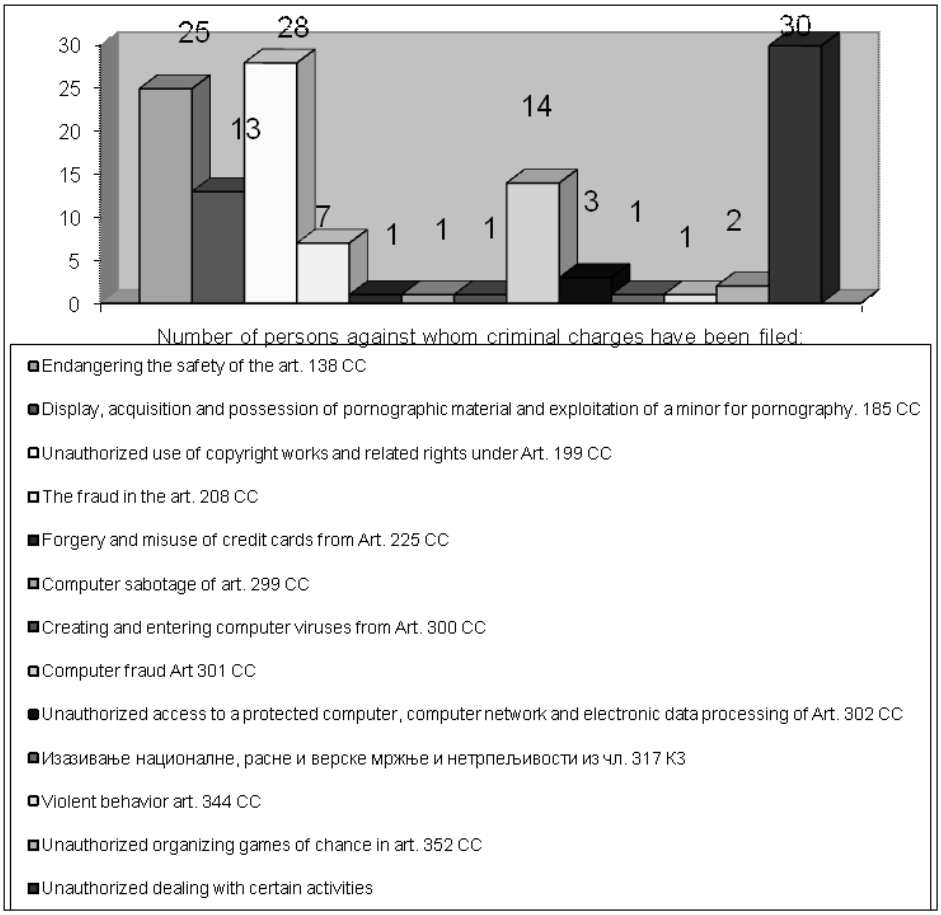
No.	The cybercrime offenses:	Number of persons against whom criminal charges have been filed:
1	Unauthorized use of copyright works and related rights under Art. 199 CC	78 persons
2	The fraud. 208 CC	5 persons
3	Computer sabotage of art. 299 CC	4 persons
4	Creating and entering computer viruses from Art. 300 CC	19 persons

5	Art of computer fraud. 301 CC	2 person
6	Unauthorized access to a protected computer, computer network and electronic data processing of Art. 302 CC	6 persons

Source: Data from the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in 2009.

Data from Table 2 presented in Chart 4 as shown below.

Chart 4: Number of persons against whom criminal charges have been filed for cybercrime offenses — 2009



Special Prosecutor for cyber crime in 2010 were filed 116 criminal charges against 127 persons.[25]

In Table 3 shows the number of persons in 2010 year and filing of criminal charges of crimes cyber crime.

Table 3: Number of persons against whom criminal charges have been filed for cybercrime offenses — 2010. year

No.	The offenses cybercrime:	Number of persons against whom criminal charges have been filed:
1	Endangering the safety of the art. 138 CC	25 Persons
2	Display, acquisition and possession of pornographic material and a minor in art from pornography. 185 CC	13 Persons
3	Unauthorized use of copyright works and related rights under Art. 199 CC	28 Persons
4	The fraud in the art. 208 CC	7 Persons
5	Forgery and misuse of credit cards from Art. 225 CC	1 Person
6	Computer sabotage of art. 299 CC	1 Person
7	Creating and entering computer viruses from Art. 300 CC	1 Person
8	Computer fraud. 301 CC	14 Persons
9	Unauthorized access to a protected computer, computer network and electronic datat. 302 CC	3 Persons
10	Inciting national, racial and religious hatred and intolerance of art. 317 CC	1 Person
11	Violent behavior of the art. 344 CC	1 Person

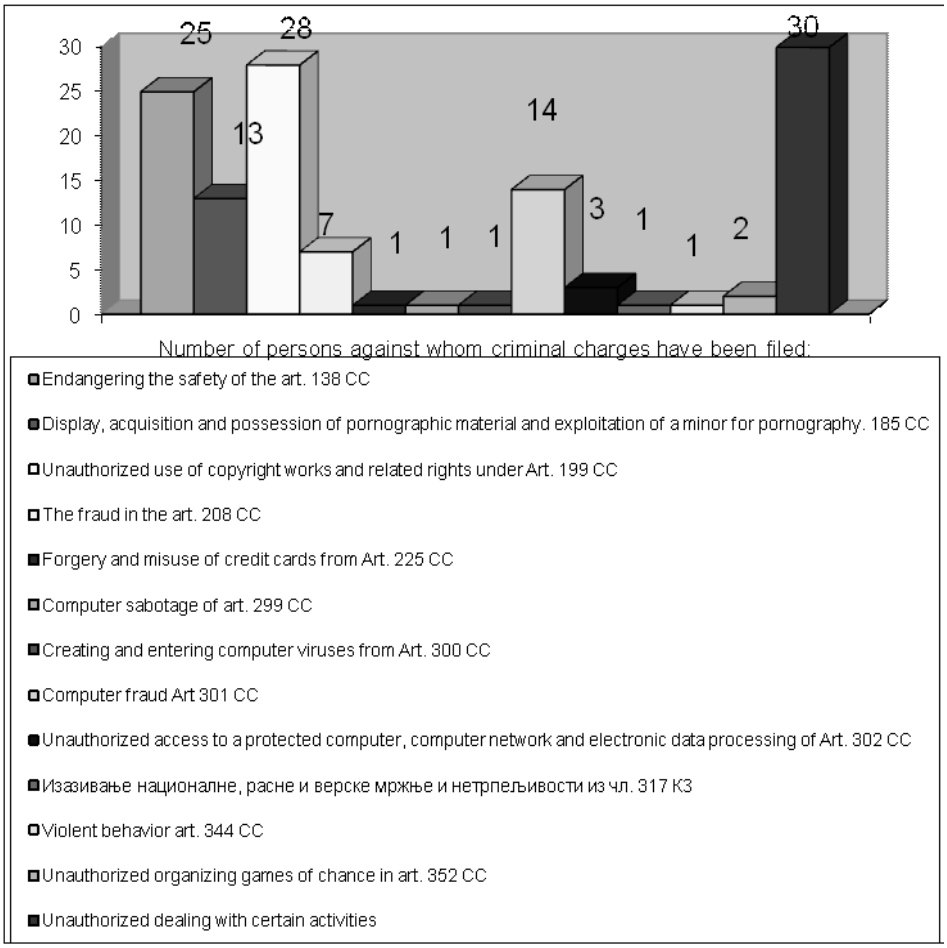
[25] Data obtained in the framework of the Report of the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in 2010.

12	Unauthorized organizing games of chance in art. 352 CC	2 Persons
13	Unauthorized dealing with certain activity article. 353 CC	30 Persons

Source: Data from the Special Prosecutor's Office for the fight against cyber crime, established in High Public Prosecutor's Office in Belgrade in 2010

Data from Table 3 presented in Chart 5 as shown below.

Graph 5: Number of persons against whom criminal charges have been filed for cybercrime offenses – 2010:



According to the representation of the number of criminal charges for the crime of computer fraud in relation to the number of criminal charges for other crimes in the area of cyber crime, reveals that in the period since 2008–2010. The growing number of computer fraud offenses detected. Namely, in 2008. 9 were filed criminal charges for this work, in 2009 were filed 19 criminal charges as in 2010. year that number was 14th Over time, this crime stands out as one of the most common abuses in the field of computer technology. Certainly by the large amount of damage caused by the harmful effects that entails, such rank and certainly deserves.

Conclusion

Although today, it is impossible to imagine the functioning of life and society the as a whole without the use of computers and modern information technology, the awareness arises that this useful and necessary funds can be used for illicit, unlawful objectives, primarily to obtain an economic benefit for any person or for causing harm to others. Since they were in Serbia until present day, recorded numerous cases of abuse of computers for criminal purposes, it is high time that the science and practice of increasingly devote to these issues. Computer scams are very common misuse of computers and other elements of computer technology. So far, caused a very large financial losses in a number of countries, and their negative effect on the Serbian territory every day more apparent. Analysis of the practice of the Special Prosecutor for cyber crime, we came to some conclusions regarding the activities of the judicial and police authorities in the field of combating this phenomenon. On the one hand, there is a rise in the number of criminal charges for the crime of computer fraud. On the other hand, the number is still very small bearing in mind that this problem is a phenomenon of modern society and each country individually. In this regard, the results of the conducted research can serve as an adequate basis for the further development and strengthening of defense mechanisms of the Republic of Serbia in the field of combating the negative consequences of computer fraud.

Bibliograpy:

1. Aleksić, Živojin and Škulić, Milan, *Crime*, Faculty of Law, University of Belgrade, Službeni Glasnik, Belgrade, 2007.
2. Banović Božidar, *Providing evidence in criminal investigations processing crime economic crime*, Police College, Belgrade – Zemun, 2002.
3. Bellour J. C.: "The International fraud", *Choice 1*, Zagreb, 1981.

4. Council of Europe, Recommendation No. R (89) 9 of the Committee of Ministers to member states on Computer-related crime, https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2
5. Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001; European Treaty Series (ETS) – No. 185; http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc(downloaded:05.08.2010.)
6. Information Corner, Interesting http://kompjuterskikriminalitet.blogspot.com/2009/02/zanimljivosti.html (downloaded: 15.09.2010.)
7. Criminal Code, Službeni Glasnik, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/09.
8. Cybercrime, APIS Security Consulting; http://www.apisgroup.org/sec.html/Knjige/UMOB/sec.html?id=29 (downloaded: 05.09.2010.)
9. Lidija Nikolić-Komlen; Radoje Gvozdenović, Saša Radulović, Aleksandar Milosavljević, Ranko Jerković; Vladan Živković; Saša Živanović, Mario Reljanović, Ivan Aleksić, *Combating cyber crime*, the Association of Public Prosecutors and Deputy Public Prosecutors of Serbia, Belgrade, 2010.
10. Pavlović, Šime: "Computer crimes in the Criminal Code — the basics of the Croatian information rights", *Croatian Annual of Criminal Law and Practice*, Vol. 10, br. 2/2003, Zagreb, 2003.
11. Computer fraud tough six million "Victory"; http://www.pobjeda.co.me/citanje.php?datum=2005-11-19&id=75425 (dowloaded: 07.05.2009.)
12. Škulić, Milan, "Computer Criminal — how to respond to the challenge", Proceedings of the Conference on computer science and information technologies YU INFO '98 program areas: legal aspects of computer science 1225–1230, Kopaonik, 1998.
13. Statistics, Fraud and deception-related crimes, Cybercrime, Australian Institute of Criminology, 2007, Canberra, http://www.aic.gov.au/statistics/hightech/cybercrime.aspx (downloaded: 12.02.2011.)
14. The Latest Cybercrime Statistics On The Internet, Tech Watch, http://www.techwatch.co.uk/2008/04/04/the-latest-cybercrime-statistics/(downloaded: 12.02.2011.).
15. Wolfgang, Heidel, "Taglich 500 Milliarden USD – Transaktionen uber EDV", *Criminalistics*, 12/1984.