Journal of Digital Science

ISSN 2686-8296

Volume 1 Issue 1 December 2019

CONTENTS

Reforming Russian legislation for crimes in the digital economy

Anna Mingaleva[1,2]

[1] GSEM, Ural Federal University named after the first President of Russia B. N. Yeltsin, Ekaterinburg, Russia
[2]Institute of Certified Specialists, Perm, Russia

https://doi.org/10.33847/2686-8296.1.1_5

Received 07.09.2019/Revised 25.10.2019/Accepted 11.12.2019/Published 22.12.2019

Abstract. The aim of this research work is to analyze Russian criminal legislation on punishment for computer crimes. The growth in the number and intensity of cyber-attacks throughout the world also leads to an increase of costs for companies and society as a whole to provide protection against cyber-attacks and to prevent losses from them. The financial sphere of the economy suffers especially. The article provides statistical and expert data on the potential damage from the suspension of the financial institution's activities, including lost profits and costs for restoring websites after cyber-attacks. A significant increase in the number of crimes committed with the help of digital devices and a multiple increase in the amount of damage from them were revealed on the basis of an empirical study. On the part of the business community, the demand for the state to toughen penalties for computer crimes is increasing. To this end, in 2018 novels were introduced into the Criminal Code of the Russian Federation, which toughened criminal liability for embezzlement of funds from bank accounts or electronic money. It is shown that the changes introduced by the legislator in the criminal legislation of Russia take into account modern threats to economic security and increase the level of protection of the financial interests of citizens, credit organizations and the state as a whole.

Keywords: economic losses, punishment, computer crimes, criminal punishment, stealing money, cyber-attacks

1. Introduction

Expanding the scope of digital technologies application in the credit and banking sector creates broad prerequisites for increasing the speed of banking operations, improving customer service, and transparency of financial transactions. However, the use of digital innovations in the financial sector of the economy carries significant criminal risks with it according to experts [1].

At the same time fraudulent actions in the field of computer information have a great public danger, as they can immediately cause damage to a significant number of citizens, as well as jeopardize the functioning of the financial and credit system due to violation of bank secrecy, destruction, blocking or modification of computer information.Cyber-attacks are ranked among the world's major threats according to the study 'Global Risks Report' prepared for the World Economic Forum in Davos.

According to the respondents' evaluation, the probability of "Cyber-attacks: Theft of data/money" increasing is 82 % (4th place in the ranking by danger level); the probability of increasing of "Cyber-attacks: disruption of operations and infrastructure" is 80 % (5th place in the ranking); the probability of increasing of "Personal identity theft" is 64 % (10th place in the ranking); the probability of increasing of "Loss of privacy (to companies)" is 63 % (13th place in the ranking) [2].

In general, according to expert estimates, the damage to the global economy from massive cyber-attacks can grow to $ 2 trillion in 2019 and to $ 3 trillion in 2020. Accordingly, companies' and society's expenses on providing protection against cyber-attacks and preventing losses from them increases. The volume of companies' global expenditures for cybersecurity will increase by 14 times by 2021 and reach approximately a trillion dollars according to forecasts of "Sberbank of Russia" [3].

In previous research we have built a macroeconomic model of the relationship between the rising cost of banking services and the rising costs of the banking sector for providing protection against cyber-attacks. Also was showed the influence of this factor on the computer security of the sector [4]. Issues of digital security in the credit and banking sphere, prospects for its development in the conditions of digitization and increased competition from new financial institutions, which are full-fledged IT companies, as well as issues of criminal punishment for computer crimes in the credit and banking sector were identified as further research directions. In this study, we will analyze the existing measures of state protection and punishment for committing computer crimes, as well as make an analysis of the necessary directions of improvement the criminal punishment for committing computer crimes in the credit and banking sector.

2. Theory and method of research

The study of the scientific and legal literature of foreign countries has shown that the criminal legislation of many countries has imposed penalties for computer crimes for a long time. Thus, in criminal law of Austria, Germany, Sweden and a number of other European countries computer fraud is singled out as an independent offense, which, as a rule, provides for stricter sanctions in comparison with the general rules on embezzlement.

Thus, the Swedish Criminal Code (Brottsbalk) specifies how to commit a crime as a sign of a qualified crime: "A person who, using false or incomplete information, changing programs, or by any other means, illegally interferes in automatic data processing or other automatic processes, benefits for themselves, while causing damage to the property of the owner, must be held accountable for fraud" [5].

The Austrian Criminal Code (Bundesgesetz) in article 148a provides liability for material damage caused in order to gain illegal benefits for the offender or a third person by influencing the processes of automated data processing using special programs, entering, modifying or deleting data or in any other way affecting data processing [6].

In the German Criminal Code (Strafgesetzbuch) computer crime is identified as property damage through influencing the result of data processing using special programs, incorrect or incomplete data, using unauthorized data or otherwise influencing the result of data processing (paragraph 263a) [7].

Comparative and bibliographic analysis are used as a method of research. The use of other methods of scientific research is difficult due to the lack of open information on the number of computer crimes and their size. Banks, credit and financial institutions hide such information. They do not allow the public and the press to find out information about the theft of money or customer databases, as this sharply undermines the confidence of customers in these banks and financial institutions. The police and crime investigation authorities also do not disclose information about such crimes, since they have a great public danger. Thus, the lack of complete, accurate and reliable information on the extent of computer crimes in the banking and financial sectors is a serious limitation for the analysis.

The results of several studies on the state of cybercrime in Russia are used as the data source. Also we use analytical reports of Positive Technologies "The market

of criminal cyberservices. 2018" [8], "How much is security?" [9]. The analysis of data from the National Computer Incident Coordination Center (NCCI) was conducted.

The sources of a comparative analysis for the study were materials from international organizations and forums, including the conclusions made in the Global Risks Report in the framework of the World Economic Forum.

3. Research

Studies in recent years have shown tremendous damage to the credit and financial sector due to the suspension for at least 1 day of work of a bank or other financial institution. Thus, it was assumed that the cost of an attack on web resources during an hour on the darknet is estimated at about $ 5, and within a day - $ 300 according to the study "How much does security cost?" of 2017 conducted by the company Positive Technologies [9, p.16].

At the same time, the damage to the financial and credit organization, which at that time could not fulfill main functions, will be hundreds and thousands of times more. Thus, the potential damage from the suspension of financial organization, including lost profits, as well as the cost of restoring websites, was estimated for certain types of cyber-attacks and the size of potential damage by institutions of credit and financial and banking sectors (see Fig. 1).

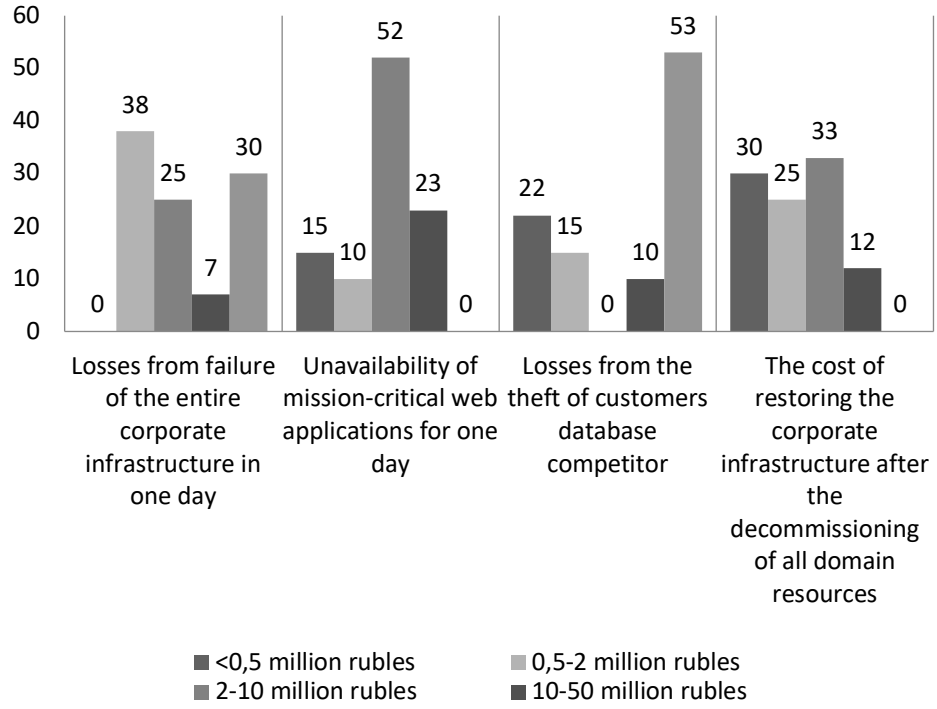

Fig. 1. Potential damage from the suspension of the financial organization, including lost profits and the cost of restoring sites

Source. Compiled by the author [9, pp.14-16, 18]

So, as can be seen on Fig. 1, the most significant are the losses of credit and financial institutions and the banking sector from various kinds of cyber-attacks (more than 50 million rubles) due to theft of customer databases (53% respondents) and in

case of failure of the entire corporate infrastructure during one day (30% respondents).The potential damage from unavailability of critical web applications in one day is estimated at 2-10 million rubles by the majority of respondents (52%). Additional costs of restoring the corporate infrastructure after the decommissioning of all domain resources in most cases do not exceed 10 million rubles. 88% of respondents called all this amount and less.

Thus, cyber-attacks targeting individual credit organizations together constitute a big threat to the entire financial sector of the country's economy. It was noted at the Insurance Technologies Forum "InnoIns-2018" held in Moscow on April 17, 2018, that 16 enterprises in Russia were being subjected to cyber-attacks every day. Business spends about $ 122.5 billion a year to protect information systems.

Theft of funds from bank accounts or electronic money seems to be attractive and profitable for criminals because of the absence of strict penalties for it. Other computer crimes against the financial and credit and banking sectors are attractive as well. What is more, computer scammers and hackers are finding new ways of committing crimes that prevent them from falling under criminal penalties.

Analysis of the methods of crimes committed in the credit and financial sphere showed that criminals continue to use social engineering methods along with the use of high-tech hacker schemes to gain access to banking systems. The most common form of such preparatory unlawful activity is pretexting, that means preliminary contact with potential victims by telephone, in instant messengers (Skype, WhatsApp, Viber, Telegram, etc.) or in social networks (VKontakte, Facebook and etc.) in order to obtain necessary information for access to the disposal of their funds. According to the position of the Central Directorate of Security and Information Protection of the Bank of Russia, the heightened danger of such criminal acts is determined by the gullibility and low level of financial literacy of the population. Consequently, in the near future, reducing the prevalence of pretexting as a preparatory activity for committing theft of money from bank accounts and electronic money seems unlikely [10]. Analysis of statistical data of law enforcement agencies showed that in 2018 citizens from 18 to 40 years old were increasingly becoming victims of "social engineers" [11].

Russian lawmakers made a number of changes in the criminal legislation of the Russian Federation considering the ever-increasing threat to society and people from committing cyber-attacks on the financial system and considering the experience of leading foreign countries in the field of criminal punishment for computer crimes in the financial and banking fields. The most important changes are shown in Table 1 [12-13].

Table 1. The most important changed in the field of criminal punishment

Article of CC of RF	**Old content [12]**	**New content [13]**
Article 158 Criminal Code of the Russian Federation (point "g" introduced by Federal Law dated 04.23.2018 N 111-ФЗ)	This basis was absent	g) Theft from a bank account in relation to electronic money (in the absence of evidence of a crime under article 159.3 of the CC of the Russian Federation) is punished: - with a fine in the amount of one hundred thousand to five hundred thousand rubles; - in the amount of the salary or other income of the convicted person for the period from one year to three years; - forced labor for up to five years with or without restriction of liberty for up to one and a half years; - imprisonment for up to six years with a fine of up to eighty thousand rubles or in the amount of wages or other income for a period of up to six months; - or without it and with a restriction of freedom for up to six years or without it.
Article 159.3 CC RF	The old name of the article "Fraud with the use of payment cards"	New title of the article "Fraud using electronic payment"
Part1 Article 159.3	Payment card fraud, that is, theft of another's property using a fake credit	Fraud with the use of electronic means of payment is punishable: - by a fine of up to

Criminal Code of the Russian Federation	payment card or a card belonging to another person by deceiving an authorized employee of a credit, trading or other organization. Fraud is punished: - with a fine of up to one hundred twenty thousand rubles; - in the amount of the salary or other income of the convicted person for a period of up to one year; - compulsory work for up to three hundred and sixty hours; - correctional work for up to one year; - restriction of liberty for up to two years; - forced labor for up to two years; - arrest for up to four months.	one hundred twenty thousand rubles; - in the amount of the salary or other income of a convicted person for a period of up to one year; - by compulsory work for up to three hundred and sixty hours; - correctional work for up to one year; - restriction of freedom for up to two years; - forced labor for up to two years; - imprisonment for up to three years.
Part 2 Article 159.3 Criminal Code of the Russian Federation	Fraud with the use of payment cards, committed by a group of people by prior agreement, as well as causing significant damage to a citizen, is punished: - with a fine of up to three hundred thousand rubles; - a convict's salary or other income for a period of up to two years; -compulsory work for four hundred and eighty hours, either by correctional labor for up to two years; -by forced labor for up to five years, with or without restriction of freedom for up to one year; - deprivation of freedom for up to four years with the restraint of liberty for up to one year or without it.	Fraud using electronic means of payment committed by a group of people in a preliminary conspiracy, as well as causing significant damage to a citizen is punished: - with a fine of up to three hundred thousand rubles; - in the amount of the wages or other income of the convicted person for a period of up to two years; - compulsory work for four hundred and eighty hours; - by correctional labor for up to two years; - by forced labor for up to five years with restriction of freedom for up to one year, or without it; - imprisonment for up to five years of restriction of liberty for up to one year, or without it.
Part 3 Article 159.3 Criminal Code of the Russian Federation	Acts, under part 1-2 of article 159.3 committed by a person using his official position, as well as on a large scale are punished: - with a fine in the amount of from one hundred thousand to five hundred thousand rubles; - in the amount of the salary or other income of the convicted person for a period of one to three years; - forced labor for up to five years with restriction of liberty for a period of up to two years without it; - imprisonment for up to five years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of a convicted person for a period of up to six months or without it; -with restriction of freedom for up to one and a half years or not.	Acts, under part 1-2 of article 159.3 committed by a person using his official position, as well as on a large scale are punished: - a fine in the amount of from one hundred thousand to five hundred thousand rubles; - or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation liberty for up to six years with a fine of up to eighty thousand rubles; -in the amount of the salary or other income of the convict for a period of up to six months or without it; - with restriction of liberty for a period of up to one and a half years or without.
Part 3 Article 159.6 Criminal Code of the Russian Federation	Acts, under part 1-2 of article 159.6 committed by a person using his official position, on a large scale are punished: a fine in the amount of from one hundred thousand to five hundred thousand rubles, or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation of liberty for up to five years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of the convict for a period of up to six months or without it; -with restriction of liberty for a period of up to one and a half years or without.	Acts, under part 1-2 of article 159.6 committed by a person using his official position, on a large scale or from a bank account, as well as in relation to electronic money are punished: a fine in the amount of from one hundred thousand to five hundred thousand rubles, or in the amount of the salary or other income of the convicted person for a period of one to three years; - by forced labor for up to five years with restriction of freedom for up to two years or without it; - deprivation of liberty for up to six years with a fine of up to eighty thousand rubles; - in the amount of the salary or other income of the convict for a period of up to six months or without it; -with restriction of liberty for a period of up to one and a half years or without.

So, the analysis of the novels of the Russian criminal legislation in the field of digital crimes introduced by the Federal Law of April 23, 2018 N 111-ФЗ "On Amendments to the Criminal Code of the Russian Federation" [14] allows speaking:

1) on expanding the field of offenses in the area of computer crimes in the banking sector to the more general concept of electronic means of payment

2) shows tougher penalties for committing crimes in the field of banking and financial activities.

Thus, under article 158 of the Criminal Code of the Russian Federation ("Theft") criminal liability is provided for theft committed from a bank account and electronic money. And the title of article 159.3 was changed from "Fraud with the use of payment cards" to "Fraud with the use of electronic payment", that greatly expands the scope of its application. Also, according to article 159.3 the severity of punishment was significantly changed:

1) the punishment for fraud with the use of electronic means of payment in the form of arrest for the time up to four months was replaced by imprisonment up to three years;

2) the threshold value of a large-scale offense was reduced from one million five hundred thousand rubles to two hundred and fifty thousand rubles.

Under article 159.6 of the Criminal Code "Fraud in the field of computer information" the new law also provides reducing the threshold value of a particularly large offense from six million rubles to one million rubles. The action assessment itself is supplemented by a new qualifying sign that is an act committed from a bank account, as well as in relation to electronic cash.

The punishment for fraud with the use of electronic means of payment, committed by an organized group or on a large scale has not changed. This type of offense is punishable by imprisonment for a term of up to ten years with a fine of up to one million rubles or in the amount of wages, or other income of the convicted person for a period of up to three years or without restriction of liberty for up to two years or without [13]. According to official judicial statistics [15], 74 and 144 people in 2017 and 47 and 33 persons during 6 months of 2018 were convicted for committing acts under articles 1593 (Fraud using electronic means of payment) and 1596 (Fraud in the field of computer information) of the Criminal Code of the Russian Federation.

National Computer Incident Coordination Center was established in July 2018 to increase the level of national computer security of the country and in accordance with part 4 of article 5 and clause 2 of part 4 of Article 6 of Federal Law No. 187-FZ of July 26, 2017 "On the Security of Critical Information Infrastructure of the Russian Federation" [16].

According to the National Computer Incident Coordination Center (NCTC), in 2018 more than 4.3 billion cyber-attacks were made on critical information infrastructure, 17 thousand of which were considered the most dangerous. This is almost two times higher as in 2017 – 2.4 billion and 12 thousand respectively.

4. Conclusions

As it was shown in the study, cyberattacks aimed at individual credit organizations together pose a tremendous threat to the entire financial sector of Russia, and financial institutions spend annually about 122.5 billion dollars to protect their information systems from hackers and scammers.

Until 2018 there were no penalties under the Russian criminal law that were adequate to the gravity of the crimes and the amount of damage from computer crimes. The absence of strict penalties makes theft of funds from bank accounts or electronic money attractive and profitable for criminals, as well as other computer crimes against the financial and credit and banking sectors.

The Federal Law dated 04.04.2018 N 111-F3 "On Amendments to the Criminal Code of the Russian Federation" and entered into force on May 4, 2018, tightened criminal liability for embezzling funds from bank accounts or electronic money.

The changes introduced by the legislator in the criminal legislation of Russia take into account modern threats to economic security and increase the level of protection of the financial interests of citizens, credit institutions and the state as a whole.

However, the application of the new criminal law against computer crimes in the financial, credit and banking sectors during the first year has showed that the adopted criminal norms are not enough to reliably prevent crimes. In addition, computer scammers and hackers are finding new ways of committing crimes that prevent them from falling under criminal penalties.

Further research in the framework of this problem is supposed to be carried out taking into account the emergence of new methods of committing computer crimes in the banking sector, the emergence of new objects of crime (for example, cryptocurrency - bitcoins, etc.) and new types of crimes.

Also, the further studies within the framework of this problem are supposed to be conducted in the context of the most important threats to Russia's digital security, including not only the credit and banking and financial sectors, but also other areas of the functioning of society.

The main limitation of the study on these issues is the lack of complete, accurate and reliable information about the size of computer crimes in the banking and financial sectors, since this information is disrupted by banks, credit and financial institutions, and the police. Such data and information are not available in official statistics.

References

1. Improving criminal liability for cybercrime in the financial sector http://ormvd.ru/pubs/102/improvement-of-measures-of-criminal-liability-for-cyber-crimes-in-the-financial-sector-of-the-econom/
2. The Global Risks Report 2019, 14th Edition, World Economic Forum, Geneva. 2019.
3. The global losses from cybercrime in 2019 can reach $ 2 trillion. - [Electronic resource] - URL: https://www.banki.ru/news/lenta/?id=10404738
4. Toropova I., Mingaleva A., Knyazev P. (2020) Macroeconomic Model of Banking Digitization Process. In: Antipova T. (eds) Integrated Science in Digital Age. ICIS 2019. Lecture Notes in Networks and Systems, vol 78. Springer, Cham. doi.org/10.1007/978-3-030-22493-6_9
5. Brottsbalk (1962: 700). Regeringskansliets rättsdatabaser. Utfärdad: 1962-12-21 Senast ändrad: 2015-04-01 Uppdaterad: t.o.m. SFS 2015: 97. https://www.legislationline.org/documents/section/criminal-codes
6. Bundesgesetz vom 23. Jänner 1974 über die mit gerichtlicher Strafe bedrohten Handlungen (Strafgesetzbuch - StGB) https://www.legislationline.org/documents/section/criminal-codes.
7. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juni 2019 (BGBl. I S. 844) geändert worden ist. https://www.legislationline.org/documents/section/criminal-codes.
8. The market for criminal cyber services. 2018. https://www.ptsecurity.com/ru-ru/research/analytics/darkweb-2018/.
9. How much is security? Analysis of information security processes in Russian companies. Positive Technologies. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf.
10. Barkhatov E.N. Features qualifications fraud in the field of computer information and its distinction from other offenses // Modern law. - 2016. - № 9. - p. 111.
11. New bank fraudsters: we are called "social engineers"! // BANKIN RUSSI. 2017 December 14th. - [Electronic resource] - URL: https://bankinrussia.ru/news/novye-bankovskie-moshenniki-socialnye-inzhenery.
12. Criminal Code of the Russian Federation. Old edition: GARANT system: http://base.garant.ru/57412609/644c26293f27715490005d21e7af011f/#ixzz5tFVlIB3l.

13. Criminal Code of the Russian Federation. New edition. GARANT system: http://base.garant.ru/57412609/644c26293f27715490005d21e7af011f/#ixzz5tFWXjg5s.
14. Federal Law of April 23, 2018 N 111-ФЗ "On Amendments to the Criminal Code of the Russian Federation" http://www.consultant.ru/document/cons_doc_LAW_296451/.
15. Summary statistics on criminal status in Russia for 2016; Summary statistics on criminal status in Russia in 2017; Summary statistics on criminal status in Russia for 6 months of 2018 // Judicial Department at the Supreme Court of the Russian Federation. - [Electronic resource] - URL: http://www.cdep.ru/index.php?id=79.
16. Order of the Federal Security Service of Russia of July 24, 2018 N 366 "About the National Coordination Center for Computer Incidents" System GARANT: http://base.garant.ru/72041506/#ixzztv1rQY2i.

Aims and Objectives
Published online by ICS two times a year, Journal of Digital Science (JDS) is an international peer-reviewed journal which aims at the latest ideas, innovations, trends, experiences and concerns in the field of digital science covering all areas of the scholarly literature of the sciences, social sciences. The main topics currently covered include: Digital Communications and Network; Digital Economics, Education, Engineering, Finance, Health Care.

The main goal of the journal is the effective dissemination of original incites/results generated by the human brain and presented/reflected in articles using modern information/digital technology.

Contact information

Journal URL: https://ics.events/journal-of-digital-science/

Email: conf@ics.events