e-journal of
Social and Legal Studies

Security and Threats of Information Society in Russia

Pavel A. KABANOV[1]
Liliya R. KHAIRUTDINOVA
Leisan BULANOVA

Abstract

It is essential to note that computer crimes are increasingly coming to light as one of the newest threats to global security. This problem has become ever more urgent for the Russian Federation over the last several decades. The primary goal of this paper is to raise awareness regarding countermeasures against cyber criminal activity. The authors of this paper invite cyber crime scholarly community and specialists of the field to contemplate the real grounded measures and mechanisms of deterring criminals from launching vigorous cyber attacks. The paper will examine how cyber crime statistics varied for the 1997 to 2014 period, and what elaborate law enforcement efforts contributed to the cyber security sector in Russia.

***Keywords**:* cybercrime, computerized information, phishing attacks, Internet technology, the Internet, legislation, Russia.

[1] Pavel A. Kabanov, Liliya R. Khairutdinova,

Kazan Innovative University named after V.G. Timiryasov (IEML),

Leisan Bulanova

Kazan National Research Technical University named after A. N. Tupolev - KAI

Authors Note

Pavel A. Kabanov, Department of Law, Kazan Innovative University named after V.G. Timiryasov (IEML), Naberezhnye Chelny, Russia; Liliya R. Khairutdinova, Department of Law, Kazan Innovative University named after V.G. Timiryasov (IEML), Naberezhnye Chelny, Russia; Leisan N. Bulanova, Department of Humanities and Social Studies, Kazan National Research Technical University named after A. N. Tupolev - KAI, Naberezhnye Chelny, Russia.

Correspondence concerning this article should be addressed to Leisan Bulanova, Department of Humanities and Social Studies, Kazan National Research Technical University named after A. N. Tupolev - KAI, Naberezhnye Chelny, Russia.

Contact: lnbulanova@mail.ru

Security and threats of information society in Russia

The problem of cybercrime during the globalization of information processes and information society development in Russia is still insufficiently developed. The Russian Federation is not in the list of States that have signed the Council of Europe Convention on Cybercrime, the latter being the only international instrument on the protection of human rights in cyberspace. Currently, Russia is not ready for full cooperation in this field with foreign partners. The international community is also in the process of developing a uniform policy in this matter, as evidenced by the ongoing work of representatives of the various states in the cybercrime fight.

Computerization has become the gateway to success in any enterprise and the revolution in information technology has spread to all spheres of human activity. It is quite obvious that technology transfer always has both positive and adverse consequences. In general, manufacturing, managerial and other aspects of the organization activity seem now infeasible without a wide implementation of advanced digital technologies. Under such circumstances new risks and threats coming along with the advances require a timely response. On the basis thereof the purpose of the study is to determine the real state of cybercrime in Russia relying upon the official statistics of the Russian Ministry of Internal Affairs and judicial practice.

Information and technological innovations significantly widen the cybercriminal field and facilitate hacker attacks efficiency. Hence cybercrime is spreading worldwide at a faster rate than any other types of crime. We have to bear in mind that the difficulties of investigating such crimes arise with the rapid advancements in information exchange speed and the constant inflow of technological innovations. Growth in internet has fostered rearranging of domestic e-crimes into transnational ones. Therefore, the matter of improving the cyber security strategy is under thorough consideration in any country across the globe. The free flow of information in cyber space adds up to both positive and negative effects on economic and social development, education and democratic governance. The rapid growth of information and communication technologies in cyberspace creates new opportunities for criminals to commit various technically perfect crimes using the vulnerability of phishing attacks programs.

The scientific value and significance of the study lies in the fact that for the first time a study of cyber crime in Russia is carried out through the analysis of statistical indicators for 1997 to 2014 period. The resulting research ensured an important insight into evaluation of the crime through quantitative indicators, reflecting its negative devastating consequences for society. Introduction of examples from the investigation practice and court hearings of crimes in the field of computer and network technologies is certainly an important and positive aspect of our research. This study may affect the formation of the common international practice of combating cyber crime.

Methods and Methodology

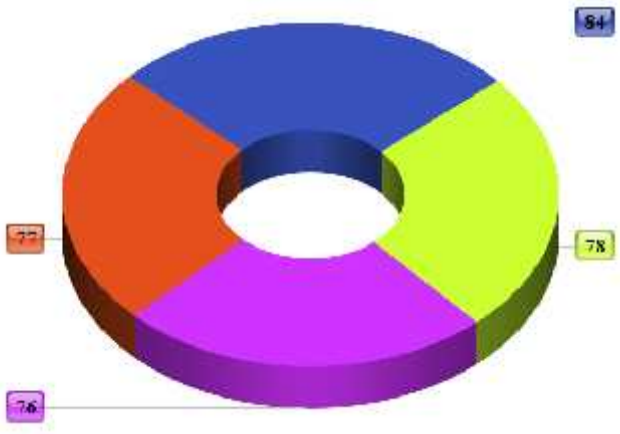
The research entails the execution of several procedures in an attempt to systematically perform a comprehensive scrutiny of the matter and subsequently introduce useful and unbiased information regarding the core issues of concern facing cyber criminologists today.

The method of analysis involved an initial review of some related works in the research area. The methodological basis of analysis involved dialectical materialism as well as such well-grounded scientific methods as a statistical, structural and comparative analysis.

Discussion

Having a massive presence as an active participant in cyberspace, Russia has been brought face to face with one of the most obvious threats. Digital war is aggravated by deliberate cyber attacks against corporations, governments and individuals (Khairutdinova, 2014). This can endanger the economic well-being as well as national and public security.

A survey conducted in Russia serves to prove that cybercrimes are among the five main types of economic crimes. The development of Internet technologies gives birth to a wide range of threats posing a real danger to the modern society due to high and climbing cyber crimes statistics on the territory of Russia. Consequently, companies are becoming more vulnerable to cyber crimes around the globe.



According to the survey 77% of respondents are concerned about the damage to reputation, 84% worry about financial losses, whereas 78% of survey participants stay anxious about intellectual property theft and 76% are nervous about instability of operating activities. The level of concern about cyber crime impact through the non-compliance to legal acts has decreased from 79% to 56%.

Cyber crime we define as a set of crimes committed in cyberspace by using computer systems or computer networks as well as other means of access to cyberspace, within the computer systems or networks, against computer systems, computer networks or the computerized data.

Halder and Jaishankar (2011) define cyber crimes as follows:

> Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS). (p.387)

To further explore this topic we need to highlight some articles that may distinguish between a fair share of cyber crime incidents. Cyber crime offending includes traditional crimes under the Criminal Code of the Russian Federation, such as theft, fraud, extremism, terrorism, copyright infringement when the illegal acts are committed using a computer and the Internet.

The Criminal Code of the Russian Federation allows for Article 272. Illegal access to computer information; Article 273. The creation, use and distribution of malicious computer programs; Article 274. Misuse of devices for storage, processing or transmission of computer information and telecommunication networks.

A subsequent comparison of the above stated articles is to extensively reflect the findings of the number of separate cyber abuse incidences for the 1997 to 2014 period. The dataset of the present study collected from official statistics by Main Information and Analysis Centre of the Russian Ministry of Internal Affairs shows that during recent years quite a few cases have been initiated against such crimes in the sphere of computerized information.

Figure 1. Crimes on illegal access to computer information

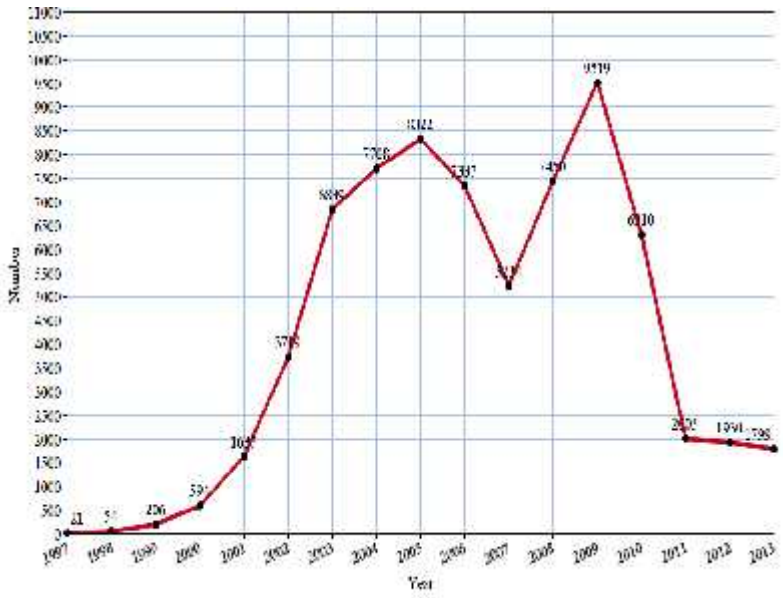


Figure 2. Crimes on creation, use and distribution of malicious computer programs

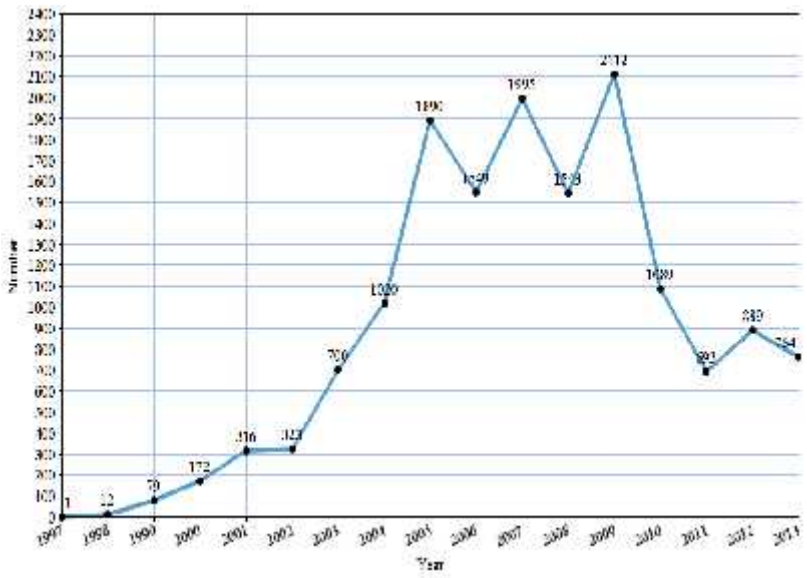


Figure 3. Crimes on misuse of devices for storage, processing or transmission of computer information and telecommunications networks

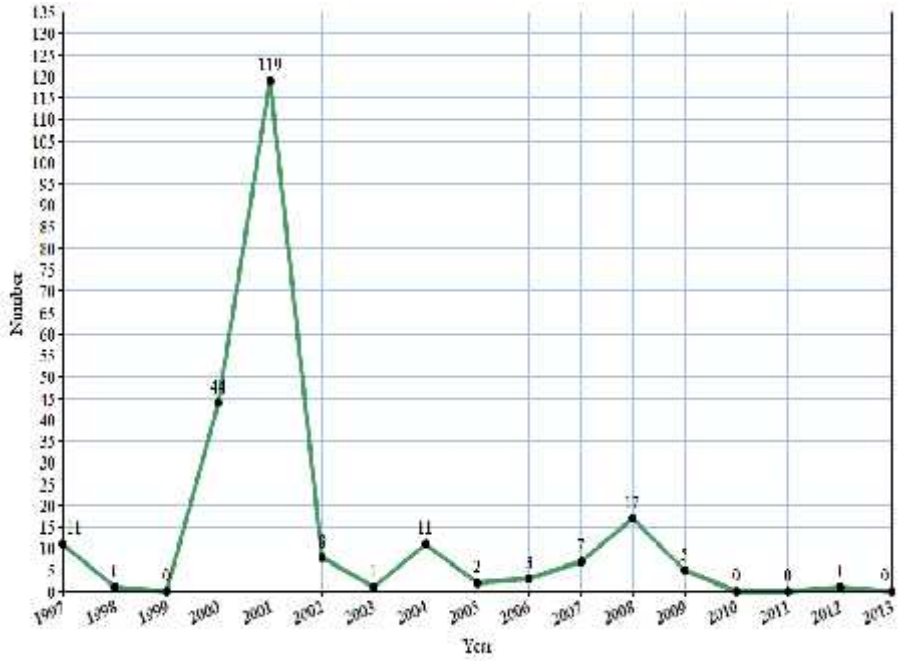
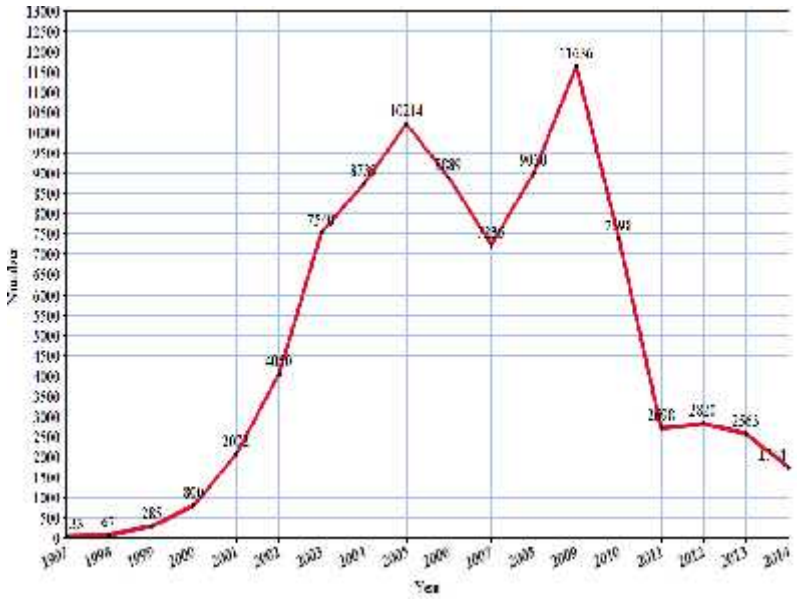


Figure 4. Amount of cyber crimes in Russia for 1997 to 2014



Analysis of statistical data on crimes in the sphere of computer information clearly shows a more than 300-time increase of the number of reported crimes in Russia for the period from 1997 to 2005, to total number amounting to about 10,000 crimes per year. Crime peak is observed in 2005. Underlying reasons of the rapid increase in cyber crime activities during this period are the intense development and spread of computer technology, lack of the Internet control, booming popularity of Internet programming, all the factors creating a breeding ground for criminal world.

A further decrease from 2006 to 2007, with the total number of cyber crimes in 2007 decreasing by 18.5% (i.e. 1653 cases) as compared to 2006, can be explained by growing

interest to security challenges and tightening of laws in the field of cybercrime. 2008 in Russia was marked by more than 14000 crimes in the sphere of information technologies, which is 2000 more crimes as compared to 2007. Total 5572 criminal cases were initiated by the Office “K” at the Russian Ministry of Internal Affairs in 2008, the number being 21.4 % more than in 2007. It is worth noting that according to the statistical data of 2008 the police submitted to the courts over 5638 criminal cases under Article 272 Illegal access to computer information, 1359 cases under Article 273 The creation, use and distribution of malicious computer programs, 8 criminal cases under Article 274 Misuse of devices for storage, processing or transmission of computer information and telecommunication networks misuse of devices for storage, processing or transmission of computer information and telecommunication networks. It is an important point to be made that within 2008 the police recorded 1078 crimes under Article 159 Fraud and initiated 620 criminal cases, which is 66% more than in 2007. In 2008 the law enforcement officials arrested criminals who were engaged in organizing distributed denial-of-service attack (DDoS-attack) on the websites of different companies and extorting money for attack termination. The infecting attacks targeted on about 8000 PCs, with more than 10 major Russian companies suffering huge losses.

As we see from the graph, cybercrime in 2009 has made a qualitative leap in the number of registered crimes, the time proving to be ripe for the Russian cybercrime market. It may be noted that cybercrime have become fashionable, whereas the police did not succeed in fighting against the anonymity and sorting out cyber-attacks. According to the study published by McAfee in January 2009 cybercriminals around the world caused trillion-dollar damage to companies all over the world. That is to say, 2009 witnessed booming cybercrime consequent to the global recession of 2009 and the global crisis as a result of the recession in the global economy that began with the crisis in the US financial sector in 2007-2008.

In 2010 we observe the growing popularity of theft in online banking systems, with the victims being mostly legal persons, whereas 2011 was a year of surge in theft from individuals. Through web injects and Trojans theft attackers redirected the user to a phishing resource. Subsequently, there was a drastic

decline in the number of registered cybercrimes from 2010 to 2011. The downward tendency observed up to 2014 and now on can be easily explained by the increased anonymity of cyber attacks, more sophisticated forms and lack of cybervictimity investigation.

The given statistics can not but gives rise to questions and overall concern among experts in the field of information security as to what extent the official statistics reflect the real scope of the existing cybercrime. The analysis of statistical data reveals 1744 cyber crimes in Russia throughout 2014, whereas only 618 perpetrators are detected (see *Table 1* below):

Table 1: Cyber crimes in Russia in 2014

Articles of Criminal Code	Number of cyber crimes detected	Number of perpetrators detected
Article 272	1154	290
Article 273	587	327
Article 274	3	1
Total	1744	618

The practice of cyber crime investigation possesses a number of peculiarities and calls for special training and techniques. The cyber crime appears to be a widely spread phenomenon, with the crimes frequency increasing considerably from year to year proportionally to the number of registered Internet users. For the past ten years (2003-2012) the number of Internet users in Russia grew approximately by 5.4 times, from 12 million in 2003 up to 59.7 million (i.e. 43% of the population) and 68 million (i.e. 48% of the population) in 2010 and 2012 accordingly. The Ministry of Mass Communications reports a dramatic increase of Internet surfers in 2014.

Irrespective of the difference in growth rates, the total number of crimes in computer technology sphere is still growing. What is even more alarming is that the tendency is typical not only of Russia, but is observed throughout the world. So we are confident in predicting the continuous growth of computer-related crime and its further technological development in the nearest future. This is confirmed

by some sources which investigated into criminal cases involving crimes based on computer technology, which determine more than 20 main ways of committing crimes in the sphere of computer information and about 40 various kinds. First and foremost, the adverse effects are caused by illegal actions of a criminal nature, i.e. the computer perpetration.

Russian criminal policy takes into account the international cyber crime rates. Using remote access to global information systems (e.g., Internet) makes it possible to insist on transnational nature of computer crimes and provides the opportunity for cybercriminals to take their efforts in overcoming the security systems of the site, portal, Web - node (computer attacks) in order to use complex criminal schemes in the credit and financial field, in creating strong informational and technological impact, distributing pornographic materials, providing assistance to addicts and committing other property and violent crimes.

High latency typical of the overall crime rate in our country is distinctly observed in cyber crime sphere. The scholars revealed a number of reasons (e.g., the information gap of Russia as compared to the leading foreign countries, imperfect legislation that allows law enforcement authorities not to attribute cyber crime offences to crimes; the lack of interest on the part of the victims in the complete thorough investigation) that intentionally provoke drastic uprising of cyber incidences in information area. (Drannikov, 2006).

Cyber threats and malware create a high-degree risk for citizens, enterprises and intellectual property, with the risk occurring through the use of unlicensed software. However, even those users who originally were not intent to violate the law by purchasing software from unknown vendors or by downloading it from unreliable sources, have great chances of becoming illegal users of malicious software, or part of a network that spreads dangerous viruses in the Internet.

The most successful countermeasures against cyber crimes are deemed to be adoption of the Federal Law “On legal protection of software and databases” dd. September 23, 1992.; adoption of the Federal Law “On information, IT development and information protection” dd. February 20, 1995; amendments to the Criminal Code of a special chapter № 28 “Crimes in the sphere of computer information”; adoption of the Federal Law № 149-FL “On information, information technologies and information protection” dd. July 27, 2006.

It is worth noting that the Federal Law “On information, IT development and information protection” coming into force on February 22, 1995 proved to be one of the first regulators for this kind of public relations. However, the period from 1992 to 1995 was marked by adopting other laws and by-laws regulating this specific relationship, i.e., the Federal Law “On Legal Protection of Software and Databases” dd. September 23, 1992; the Federal Law “On Copyright and Related Rights” dd. July 9,

1993; the Federal Law "On information, IT development and information protection" dd. July 21, 1993 etc.

Aiming at detection, investigation, apprehension and prosecution, Russia is struggling to employ various effective countermeasures against cyber attacks. Of great importance are:

- the "Information Security Doctrine of the Russian Federation" and "Principles of State Policy of the Russian Federation in the field of international information security for the period up to 2020" approved by V. Putin. The latter principles are designed to boost the foreign policy of the Russian Federation in the way of reaching an agreement and mutual interest in the process of internationalizing the global information space.

- the Federal Law № 149-FL "On information, information technologies and information protection" enacted by government on July 27, 2006.

- "Guidelines for the implementation of prosecutorial supervision over implementation of laws in the investigation of crimes in the sphere of computer information" developed and adopted by the Russian General Prosecutor's Office.

The government created the Interdepartmental Commission for the Protection of State Secrets, the commission being a collegial body coordinating the activities of public authorities for the protection of state secrets with the view of development and implementation of government programs and regulatory guidance documents to ensure exercising the legislation of the Russian Federation.

There is the federal government agency authorized in the field of security (Federal Security Service), the federal government agency authorized in the field of defense (Ministry of Defence), the federal government agency authorized in the field of foreign intelligence (Foreign Intelligence Service), the federal government agency authorized in the field of counteraction to technical intelligence and technical protection of information, and their territorial authorities (Federal Service for Technical and Export Control); public authorities, enterprises, institutions and organizations and their official secrets protection units.

There are special units to carefully combat cyber crimes in Russia, i.e. the Office "K" at the Russian Ministry of Internal Affairs.

Examples of cyber crimes and offenders

We should highlight the most common offenses related to violation of the law in the field of computer information:

Two brothers from St. Petersburg: The first case of computer phishing in Russia

A group of young people has been accused of committing crimes under Part 2 of Article 272, Part 1 of Article 273, Part 4 of Article 159 of the Criminal Code (illegal access to computer information, use and distribution of malicious programs for computer technology, collusive fraud committed by a group of persons with causing damage in especially big amount).

Having studied the information on specialized internet forums and basic principles of the e-banking, two brothers from St. Petersburg developed a plan aimed at theft of funds from customer accounts in one of the largest Russian banks.

The brothers hired a student from Kaliningrad to develop a fake of the original remote banking service web page. On this fake website hackers placed their leased telephone numbers for technical support. Moreover young people applied a number of malicious programs (e.g., Trojan), which after activation on an infected computer modified or substituted some of the parameters in the bank-client functioning.

As a result, any referral of clients to the banking site was redirected to a fake web page belonging to hackers. So the customers entered their personal data (a unique number, a password and a variable code required for cash transactions). This information was saved by virus software, then processed and sent to hackers.

In order to get new variables codes, the attackers called clients or sent SMS messages stating the need to re-enter the variable code. Then the hackers on behalf of the clients sent remote orders to transfer funds from their bank accounts to the third parties' accounts and cashed the money afterwards.

Thus, from May 2010 to February 2011 the criminals deceived more than 140 citizens from 46 regions of Russia and took possession of their funds in the total amount of 13 million rubles.

N.Malygin: copyright infringement

In August 2015 the Oktyabrsky District Court of Kirov ruled on the case №1-359/2015 against N.Malygin, who being motivated by lucrative impulse and having criminal intent for unlawful use of intellectual property, posted an advertisement on the «Avito.ru» website proposing a fee-based computer installation of unlicensed software. N.Maligin illegally used copyrighted works, as well as stored and transported counterfeit copies of works in especially big amounts for further marketing.

His illegal access to law-protected computer information resulted in blocking and alteration the latter.

He distributed and used computer programs being deliberately designed to block unauthorized modification of computer information and neutralize the protection of computer information.

Thus, N.Malygin within the period from March 17, 2015 to April 1, 2015 unlawfully stored and transported counterfeit copies of computer works the owners of which are the corporations of «Microsoft» and «Autodesk Inc.», with the total damage amounting to 677 876 rubles 95 kopecks.

A young man from Irkutsk: Trojan virus and fraud

The Oktyabrsky District Court of Irkutsk ruled on the case against the Internet user who stole more than half a million rubles from the accounts of brokerage companies' clients by sending an e-mail with a Trojan virus. He was convicted of Part 2 Article 273 (distribution of malicious software which caused major damage), Part 2 Article 272 (illegal access to computer information), Part 3 Article 159 (fraud in especially big amount), item in Part 2 Article 158 of the Criminal Code (theft with causing significant damage).

The young man bought the "Trojan virus" program from the Internet and sent it in an attached letter to one of the e-mail addresses. When the recipient opened the message, an attacker could gain access to all the information on the infected computer. So the sender of the letter could obtain logins and passwords to personal cabinets in brokerage companies, investment project site as well as billing information of the depositors. Using these data the offender stole more than 600 000 rubles.

The young man pleaded guilty and actively promoted the investigation of the crime. The court sentenced him to 2.5 years of imprisonment with a three-year's probation period.

Alexei Petrochenkov: Trustee Payment

Lyubertsy City Court ruled a case against Alexei Petrochenkov who matched logins and passwords to the accounts of several Internet subscribers and for a long time enjoyed a free access to the network under their names. He was convicted of Part 2 Article 272 of the Criminal Code (illegal access to computer information).

On one of the sites Petrochenkov discovered that the accounts of subscribers of Internet providers are identical: the caller's name contains characters followed by the four digits – a personal phone number and a default password of the provider. With sufficient knowledge in the field of IT, he matched a username and password to the account of a casual user and activated his personal office service "Trustee Payment". Likewise he was given access to the accounts of several other users and from October 2013 to August 2014 used the Internet at their expense.

Alexei Petrochenkov pleaded guilty and was sentenced to one year of corrective labor, with 10% withholding from his earnings.

The accomplices from Moscow and Yekaterinburg: hacker attacks

Hackers from Moscow and Yekaterinburg decided to go into hacker attacks business. Placing the advertisements they concealed their true IP-addressed and used a variety of network anonymizers. The potential clients got in touch with them through e-mail and instant messaging. The orders were paid only through electronic payment systems. The cost ranged from 3 000 rubles up to 10 000 rubles, depending on the size and complexity of the performed services. The accomplices carried out from 30 to 40 orders a month. Their customers were individuals or legal entities longing for confidential information about potential victim privacy and trade secrets of enterprises and organizations. Regular clients were even provided certain discounts.

The hackers were convicted of Article 272 of the Criminal Code (illegal access to computer information).

Skimmers and skimming devices

Two skimmers from the Kaluga region with the help of special equipment disguised as ATM lighting collected data on eight hundred credit cards.

Obninsk City Court found the 32- and 33-year-old Moldovan citizens guilty of Part 3 Article 183 of the Criminal Code (illegal collection of information constituting bank secrecy and causing major damage), Part 3 Article 272 of the Criminal Code (collusive illegal access to law-protected computer information with causing major damage), Part 3 Article 30, item B in Part 4 Article 158 of the Criminal Code (collusive attempt to steal in especially big amount).

From March to June 2014 the accomplices arrived in Obninsk to set skimming devices to ATMs of Sberbank of Russia. The devices were equipped with miniature video camera module, which resembled regular lighting but was intended to capture the input PIN of payment cards. In addition, the criminals installed special equipment which enabled them to read the data from card magnetic stripes. On the whole they got hold of the data from 850 payment cards, the accounts of which were more than 21 million rubles. The accomplices managed to steal only 1.3 million rubles and were sentenced to six and seven years of standard regime penal colony.

Banks: longing for illicit enrichment hackers seek access to client information

Thus, on March 5, 2016 “Metallinvestbank”, “Russian International Bank” and other four credit institutions were attacked by cybercriminals. Earlier the Russian Federal Security Service along with Ministry of Internal Affairs ceased the activity of hackers’ band having stolen 1.7 billion roubles from the bank accounts by way of Trojan virus Lurk, the latter enabling remote access to remote banking system. “Metallinvestbank ranking among top 100 incurred losses for 680 million roubles. Other banks subjected to hacker attacks are outside the top 100.

The cyber security service organization of Sberbank repulsed the attack on one of its subsidiaries and forwarded the case materials to the Ministry of Internal Affairs and the Federal Security Service. Due to the initiated special operation 50 people were detained and almost half of them were sent to metropolitan pre-trial detention centers. Careful searches confirmed the involvement of the suspects in creation of infected computer botnets, targeted attacks on the bank infrastructure and money theft. According to the official representative of the Ministry of Internal Affairs, members of the band carried out at least 18 targeted attacks on bank customers’ workstations, with the total damage caused exceeding 3 billion roubles.

The high level of cyber crime in Russia in 2015 produced really disastrous consequences for the Russian economy.

According to a joint study of the Development Fund of Internet initiatives, Microsoft and Group-IB, cybercriminals caused 203.3 billion roubles damage to the economy in 2015, which is 0.25% of the total Russia’s GDP.

The damage caused by hackers is actually half of all the money allocated in 2014 to support public health, or more than 200% of the money that the government sent to the support of the media.

Dozens of Russian banks were subject to hacker attacks, organized by sending malicious messages to electronic addresses of employees in 2015.

Within the period from 2012 to 2015 the law enforcement agencies of different countries arrested 160 Russian-speaking hackers, who were involved in the theft of money worldwide using malicious programs. In Russia, the arrests with the participation of the Federal Security Service and the police took place in Moscow, St. Petersburg, Chelyabinsk and Arkhangelsk. However, the number of arrests and sentences is a far cry from the amount of unsolved cybercrimes.

Russian-speaking hackers organized an attack on Energobank Kazan in February 2015. Introducing a virus called Corkow Trojan, they broke through the bank defense and placed more than $ 500 million at non-market rates. This affected the stock exchange and changed the rouble-dollar rate by 15%.

The US National Security Agency (NSA) is closely monitoring cyberspace activity of Russia,

China, Iran and North Korea. The head of the NSA, Michael Rogers in his report of April 5, 2016 assumed that Russia crowds the top of the list among countries producing the most serious threat.

Rogers (2016) notes the following:

> The states that we watch most closely in cyberspace remain Russia, China, Iran, and North Korea. Russia has very capable cyber operators who can and do work with speed, precision, and stealth. Russia is also home to a substantial segment of the world's most 4 sophisticated cyber criminals, who have found victims all over the world. We believe there is some overlap between the state-sponsored and criminal elements in cyberspace, which is of concern because Russian actions have posed challenges to the international order. (p.3-4).

Conclusions and Future Study

Cyberspace has led to a significant increase in international cooperation. Thus a remarkable feature of cyber crimes is their transnational nature. Nowadays the borders between countries, the distances and the differences in language are really insignificant. Much attention now is given to the level of society computerization, access to computers and specialized knowledge common for programmers around the globe. Hence an immediate and useful consequence is the unanimity of law regulations on cybercrime and the need for constant recourse to foreign experience of cyber crimes fighting when creating national legislation.

Today, the Internet and social networks are the ideal sphere of activity for cyber criminals, since current information technologies guarantee criminals not only anonymity, but also provide unique opportunities to develop their activities in the social, political and economic spheres. The initial development of legislation concerning legal relations in the Internet gives the criminals more chances to develop new forms of cybercrime. Digitalized crimes make the solutions cumbersome or in some cases, even infeasible to find.

Cyber crime is on the rise, with cyber attacks becoming more vigorous and ingenious. And we are sure to predict a proliferation of instances of cyber crime from now on.

Thus most importantly, there is a need to reconsider legislation of Russia with new legal acts that can add precision and clarity to the unstable legal regulation in the sphere of computer technologies. Even a relatively small investigation into the causes of cyber crime produced from the perspective of the modern criminal policy and doctrine of Russia's information security easily confirms the urgent need for in-depth analysis of cyber crime recurrent and its notably essential components. It is our firm belief that the statistical approach to studying and reporting computer crimes is to be reviewed.

References

Drannikov, V.N. (2006). Some determinants of computer crime in the light of modern criminal policy. *Advanced information technologies and intelligent systems*, 4, 114-116.

Halder, D., & Jaishankar, K. (2011b). Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India. Victims and Offender, 6(4), 386-398.

Khairutdinova, L.R. (2014). Corruption Cybercrime in virtualized space. *Politics, State and Law*, 4. Retrieved October 16, 2015. Retrieved from http://politika.snauka.ru/2014/04/1583.

Statement of Admiral Michael S. Rogers Commander United States Cyber Command before the Senate Armed services Committee 5 April 2016. Retrieved from

http://www.armed-services.senate.gov/imo/media/doc/Rogers_04-05-16.pdf.