Leading Issues in Cybercrime: A Comparison of Russia and Japan

Nikita Simonov*
International Market Institute
Samara University of Public Administration
Aksakova str. 21, 443030 Samara
Russian Federation
e-mail: nik.s.simonov@gmail.com

Olga Klenkina
International Market Institute
Samara University of Public Administration
Aksakova str. 21, 443030 Samara
Russian Federation
e-mail: olga.v.klenkina@gmail.com

Elena Shikhanova
Samara National Research University
Moskovskoye shosse 34, Samara 443086
Russian Federation
e-mail: elen69295@rambler.ru

Abstract Nowadays, the pace of high technologies is going quick which causes a number of problems in the information sphere. Along with the globalization of the information space and digitalization, there are more opportunities for abuse in the information sphere. The reason for the popularity and rapid growth of cybercrime is its high profitability, as well as the lack of high risk. The purpose of our study is to identify the characteristics of cybercrime in the Russian Federation and Japan and to identify possible vectors of cooperation.

The experience of Japan will be useful to Russia since the problems that arise today are partly new to Russia, but already resolved in Japan. Along with this, it should be noted that the experience of the development of the Russian Federation could be used by Japanese law enforcement agencies in order to prevent unlawful attacks by our compatriots.

We see the following vectors of cooperation to comprehensively counter the cybercrime of the Russia and Japan: to unify the criminal law on cybercrime; to fine-tune law enforcement cooperation in the investigation of cybercrimes; to develop a mechanism for resolving jurisdictional issues in cyberspace.

Keywords: *digital technologies, cybercrime, leadership, globalization, Russia, Japan*

1 Introduction

In today's modern world, the law of high technologies is developing rapidly, people rely on computers and "smart devices" more often, which causes many issues in the information sphere. Along with the globalization of the information space and digitalization, there are more opportunities for abuse. The reason for the popularity and rapid growth of cybercrime is its high profitability, as well as the lack of high risk. Money that cybercriminals get for some minutes can exceed millions of dollars.

Recently, in Russia alone, more than 10,000 new cybercrimes are recorded every year (Al Azzam 2019). Cybercrime is also gaining serious scale in Japan. Basically, computer abusers hack insufficiently protected cryptocurrency wallets of users and credit cards, transfer funds to other accounts, and then it is impossible to track them.

The carried out content analysis of research on cybercrime and statistics has revealed common problems in identifying and investigating such trespasses: 1) cross-border, which is expressed in extraterritoriality of the crime, the offender and the injured party; 2) the involvement of IT-specialists to identify and investigate crimes; 3) the complexity of qualifications in accordance with the national law.

The purpose of the present study is to develop the recommendations on mutual cooperation in the sphere of cybercrime in Russia and Japan. In accordance with what, the following tasks are supposed to be solved: 1) concretization of the “cybercrime” concept; 2) analysis of current trends in the development of cybercrime in Russia and Japan; 3) determination of the vectors of mutual cooperation between Russia and Japan.

2. Literature review

In different times many authors carried out analyses of problems connected with cybercrime, which we study in our research as well, they are: Borodkina et al. (2018); Christou and Nitta.(2018); Morozov (2016); Valko (2016) and others. In addition, such researchers as Al Azzam (2019); Lakomov (2019); Schjolberg and Ghernaouti-Helie (2011), studied the modern trends of the cybercrime in the world and adequate ways of cooperation.

It should be noted that in the framework of this work the findings and conclusions on the theoretical and practical problems of computer crimes in Japan made by Morozov (2014) were fundamental to us. Furthermore, we closely examined the works on the relevance of the Japanese experience and cooperation with this country written by Borodkina and Pavluyk (2018); Broadhurst and Chang (2013); Christou and Nitta (2018); Gady (2017); Kallender and Hughes (2017). We paid attention to the geography of the sources of cyberattacks presented by NTT Group, the largest telecommunications company in Japan, in the work of Valko (2016).

Previously, some authors (Talipova 2016; Zhuravlenko and Shvedova 2015 and others) already noted the particular nature of such kind of offences and the necessity of international cooperation for many times. However, almost everyone points out that it is impossible to study the problem in its entirety due to the lack of necessary resources and information. We are of the opinion that the research on the interaction types between Russia and Japan which has technical and information potential is future oriented.

2. Methods of assessment

In the course of the study, we applied a set of methods that were adequate to the subject of the study: theoretical analysis of philosophical, legal, and sociological literature on the research topic; content analysis of legal acts and statistics on the identification and investigation of cybercrimes; analysis of law enforcement experience in Russia and Japan.

3. Cybercrime in legal doctrine

At present, there is no universally accepted definition of the term “cybercrime” and the term is not fixed at the legislative level. After analysing international acts, we can conclude that the concept of “cybercrime” is not fixed in them, and there is not a universally recognized definition. Parties to the Budapest Convention on Computer Crimes (Borodkina et al 2018), among them Russia and Japan, defined several terms in it: “computer system”, “electronic data”, “flow data”, which is not enough for a joint international fight against cybercrimes. However, an attempt has already been made in this document to classify cybercrime according to the subject of the crime and the object of the offense (Fig 1). In the classification there are four blocks with the types of crimes.

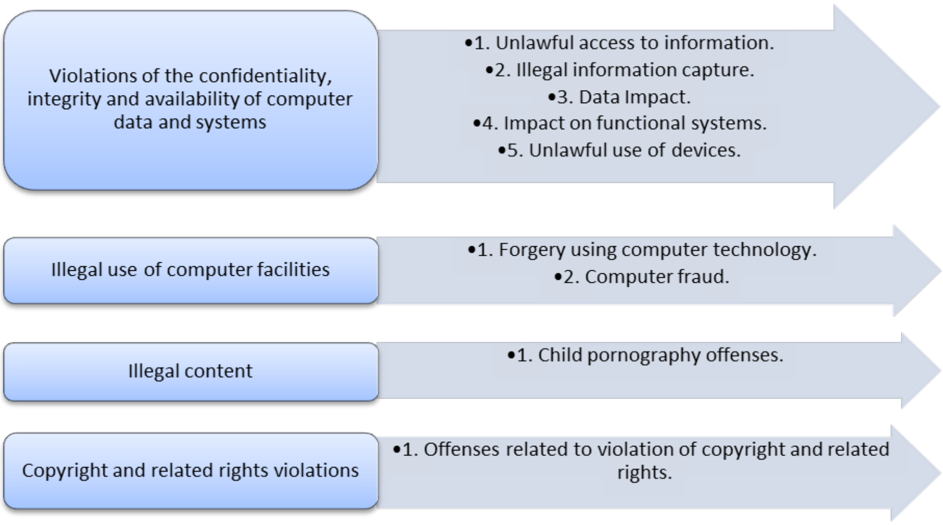

Violations of the confidentiality, integrity and availability of computer data and systems
•1. Unlawful access to information.
•2. Illegal information capture.
•3. Data Impact.
•4. Impact on functional systems.
•5. Unlawful use of devices.
Illegal use of computer facilities
•1. Forgery using computer technology.
•2. Computer fraud.
Illegal content
•1. Child pornography offenses.
Copyright and related rights violations
•1. Offenses related to violation of copyright and related rights.

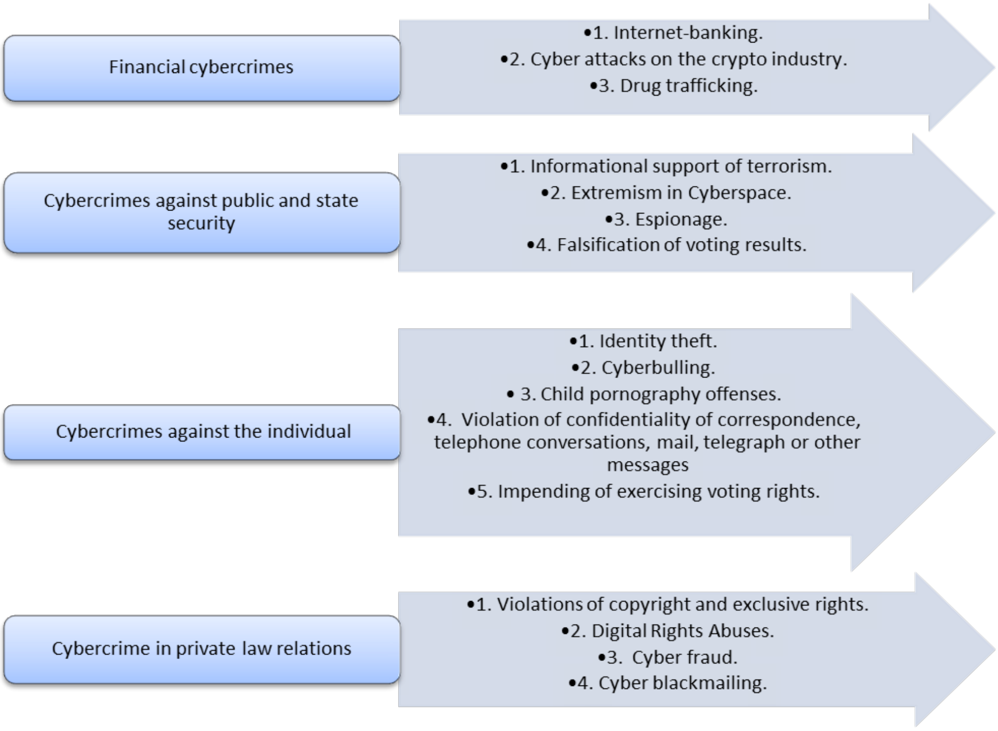
Fig 1. Classification of cybercrimes
Source: Budapest Computer Crimes Convention (2001)

The largest number is reflected in the block "crimes against confidentiality, integrity and accessibility of computer data and systems". We assume that crimes in this block are most often committed, since most cybercrimes occur directly in cyberspace.

Based on the classification of computer crimes set forth in the Budapest Computer Crimes Convention (Borodkina et al 2018), we propose to define "cybercrime" as unlawful acts against the confidentiality, integrity and accessibility of computer data and systems, as well as unlawful acts related to the use of computer tools, with copyright infringement and related rights.

It should be noted that the Budapest Convention was signed in 2001 and research in the field of cybercrime has taken a significant step forward. Moreover, the progress of information technology in different countries has left its mark on national legislation. Absolutely previously unknown technologies and means appeared both in the material and in the virtual world. In this connection, the proposed classification of cybercrimes and the definition arising from it seem outdated.

Let us turn to the legal doctrine. Among scientists, crimes committed with the help of information technologies in the virtual space are called differently: high-tech crimes, digital crimes, information crimes, computer crimes. In our opinion, the concept of "cybercrime" is broader than the concept of "computer crime". Nomokonov and Tropina (2012) initially proposed to expand the list of devices that may be used in cybercrime, including computers, other information technologies and global networks. Osipenko (2009) localizing the definition to the level of national legislation, offers to understand cybercrime as "socially dangerous acts provided for by criminal law committed on the basis of remote access to an object of abuse using global computer networks as the main means of achieving a goal". According to our reckoning to solve the problem that we stated, the most appropriate definition is one proposed by Karpova (2014): "cybercrime is an act of social deviation with the aim of causing economic, political, moral, ideological, cultural and other types of damage to an individual, organization or state through any technical means with Internet access". Based on that definition, we propose to understand cybercrime as unlawful activity in the virtual space using technical means and information technologies, prohibited by both national and international laws. Along with this, it seems possible to make more specific the classification of cybercrime proposed in the Convention (Fig 2).


Financial cybercrimes

•1. Internet-banking.
•2. Cyber attacks on the crypto industry.
•3. Drug trafficking.

Cybercrimes against public and state security

•1. Informational support of terrorism.
•2. Extremism in Cyberspace.
•3. Espionage.
•4. Falsification of voting results.

Cybercrimes against the individual

•1. Identity theft.
•2. Cyberbulling.
• 3. Child pornography offenses.
•4. Violation of confidentiality of correspondence, telephone conversations, mail, telegraph or other messages
•5. Impending of exercising voting rights.

Cybercrime in private law relations

•1. Violations of copyright and exclusive rights.
•2. Digital Rights Abuses.
•3. Cyber fraud.
•4. Cyber blackmailing.

Fig 2. Classification of cybercrime
Source: Own results

The classification contains four blocks of crimes, divided depending on the object of assault. Financial cybercrimes are aimed at public relations related to the formation, distribution, and use of illegally obtained funds. At first glance, a dispute may arise regarding the fact that drug trafficking is placed in this group of classification. However, the authors included this type of offenses deliberately, in this case we are not talking about an encroachment on the subject's health, but about the damage that this activity causes to the economies of different countries every year, about the financial flow that goes into the shadow economy through this activity.

Cybercrimes against public and state security are aimed at creating a threat and damaging the security of society and the state, in this regard they include information support of terrorism, extremism in cyberspace, espionage and falsification of voting results. It should be noted that the reported offenses committed even in relation to one country may cause damage to other participants in international alliances.

Cybercrimes against the individual are aimed at undermining social relations that ensure the security of a person in cyberspace. In our opinion, this block may include: cyberbullying in its various manifestations; in the light of digitalization of elections, current impeding of the exercise of voting rights; frequently committed identity theft and violation of the secrecy of correspondence, telephone conversations and other means of communication; and crimes related to child pornography.

Cybercrime in private law relations trespass against the interests of individuals. In particular, a change in Russian legislation regarding the legal regulation of the concept of “digital rights” made it possible to “legalize” the theft of virtual objects. We are aware that this did not provide a mechanism for investigating such crimes, but this is already a big step towards unifying law enforcement practice. In the same group there are crimes related to violation of copyright and exclusive rights, which, despite the rather long period of their existence, also do not have a single law enforcement practice. Cyber fraud and cyber blackmailing are the most popular types of cybercrime according to the statistics compiled not only by the General Prosecutor's Office of the Russian Federation (Russian Federation Prosecutor General 2020), but also by all analytical centres of international level. Further we will examine certain types of cybercrime in more detail.

4. Trends in the development of cybersecurity

According to the American Centre for Strategic Studies, the global economy is losing over $ 500 billion from cybercrime, which exceeds even the amount received from drug trafficking, which is one of the highest in the world (Morozov 2014). Judging by the emerging trend, these amounts will only increase, this is a threat to the security and economic well-being of any state.

Crimes in Internet are a new and rapidly developing area of activity for criminals. Hacker attacks are becoming more professional and difficult to spot. Juniper Research (Group-IB 2020) an analyst James Moar points out that most cyber-attacks target PCs, not mobile devices or “Internet of Things”. It is unprofitable for cybercriminals to develop the necessary tools for a cyber-attack on the Internet of Things (IoT) devices since there is no way to immediately withdraw funds in such an attack.

It should be noted that small and medium-sized enterprises become victims in cybercrimes of the commercial sector, since there are no highly qualified employees in the state, and a small budget does not allow ensuring high-quality information security. Unlike small and medium-sized businesses, large businesses cannot neglect information security, because there is constant competitive pressure from the market. Companies need to define cyber security as an essential element of their development in order to be able to prevent cyber-attacks.

Internet banking remains one of the leaders among cybercrimes. Banks are attractive to hackers because they can quickly get money. Digital technologies, on the one hand, have reduced the costs of the financial sector, and on the other hand, have increased the risks of hacker attacks with vulnerable financial security in banks. Popular online banking service requires comprehensive protection against Trojans and phishing to stay ahead of hackers to prevent theft of confidential information.

We observe a new trend of the transition of cyber-attacks from banks to the crypto industry - ICOs, exchanges, funds, wallets. We should not think that fraudulent actions regarding crypto currencies are simple, as this requires appropriate professional knowledge and technical capabilities; however, we note that in the legal sense, the owners of such assets are vulnerable. This is facilitated by the already popular anonymity of participants in crypto relations, which increases the complexity of identifying the offender and holding him accountable by law enforcement agencies. Despite the absence of a legislative regulation of cryptocurrencies, bitcoins are in civil circulation. They are not difficult to exchange for the traditional currency in many exchange offices in several countries.

Cyber openness is “fundamental” along with other trends. Today, there are precedents of attempts to commit cybercrime according to the instructions when offenders use the downloaded from the site or purchased the algorithm of actions to hack an account or commit another trespass. This suggests that people without special technical skills go into cybercrime. Today, everyone can purchase the necessary tools on the Internet and commit technically complex crimes. On the Internet, such tools are even leased. Hackers are increasingly publishing open code of malevolent software, and the Shadow Brokers group (Juniper Research 2020) has made many cyber-attack tools publicly available.

It should be noted that there has been an increase in the number and scale of cybercrime; today such crimes are already superior to those committed in the traditional way. Certainly, the damage from them is increasing. The growing number of fraudsters, the emergence of new tools for committing cybercrimes is fuelling this trend due to the lack of compliance with digital security standards by legal entities and individuals. However, it is noted that in a large number of cybercrimes, hackers use proven, outdated technologies, and it is possible to protect themselves from them, but due to the digital illiteracy of the population, even such technologies continue to cause damage. Moreover, the availability of gadgets among the population of absolutely all ages, the growing popularity of information services, and the rejuvenation of users of such services leads to the formation of a huge amount of data that becomes the target of hackers. Here, it is worth noting the role of social networks in the cybercrime growth. Due to the popularity of social networks among people, they are becoming more attractive for cybercriminals. Access to such networks allows them to steal data and commit online fraud, sell information to interested parties, and blackmail the victim.

According to the expert opinion about the cyber security conditions, of all cybercrimes, the most rapidly growing crimes are using ransomware. According to forecasts, the damage from them in 2021 will be 57 times more than in 2015. In this context, cybercrime through ransomware in the health sector deserves special attention. Outdated technologies in this area, the lack of qualified personnel in the field of cybersecurity, allow theft of personal data - medical information about a person that is valued more on the black market than financial information.

5. Vectors of mutual cooperation

As we noted earlier, it is necessary to join forces to combat cybercrime effectively. In connection with the globalization of information processes, an increase in the volume of telecommunication networks, more and more international organizations are being created in the world to combat cybercrime. The best-known alliance is the International Multilateral Partnership Against Cyber Threats (IMPACT), the UN executive cyber security authority. The organization unites states, non-governmental organizations, experts in the field of information security. In 2011, the International Cyber Security Alliance (ICSPA) was created, comprising law enforcement agencies, international business, and the governments of most countries of the world. It should be noted that with the existence of such organizations, there is still no well-established international cooperation between law enforcement agencies, and it should be also highlighted that hackers have more perfect international cooperation.

Since the 70s, Japanese experts in the field of criminal law have talked about the need to improve legislation and train qualified personnel in the field of information security, and since the 1990s, they have introduced the retraining and advanced training programs for law enforcement officials. In comparison, in the Russian Federation in modern conditions, not all law enforcement agencies have established special departments, in educational institutions the discipline of “Internet law” is only on the way to establishment.

Some researchers (e.g. Morozov 2014) point out that the national legislation of Japan has a classification of cybercrime, providing a means of determining a specific type of crime in the high technology area and keeping statistics on it. It seems necessary to globalize such work, which will eliminate the contradictions in the qualification of cybercrime in other countries with the participation of the Japanese side, which creates problems of international cooperation in the fight against cybercrime and leads to the growth of such crimes.

The experience of Japan will be useful to Russia, since the problems that arise today are partly new to Russia, but already resolved in Japan. Along with this, it should be noted that the Russian experience can be used by Japanese law enforcement agencies to prevent unlawful attacks made by our compatriots. It is noteworthy that the social, economic, political stability and predictability of Russia is important for Japan, as this is the basis for mutually beneficial cooperation. Thus, applying of Japanese experience in Russia is not only possible, but also mutually beneficial.

6. Conclusions

Summarizing the results of the study, we indicate that the lack of a fixed concept of “cybercrime” at the international level impedes international cooperation in this area. In the course of the study, we identified the following trends in the development of cybercrime: small and medium-sized businesses are the most vulnerable, cyber-attacks go from banks to the crypto industry, the development of cyber openness led to increase of the computer crime volume, and the fastest growth of crimes using ransomware is observed. The experience of international cooperation in combating crimes in cyberspace shows that international organizations are actively working, but, nevertheless, there is no established international cooperation between law enforcement agencies.

Hence, it follows that no state can fully protect itself from cybercrime, taking measures only at the national level. To comprehensively counter the cybercrime of Russia and Japan, we see the following vectors of cooperation: unify the criminal law on cybercrime; adjust law enforcement cooperation in the investigation of cybercrimes; develop a mechanism for resolving jurisdictional issues in cyberspace.

The results of the research can be used to study the trends of cybercrime and international experience in combating it. The conclusions drawn are the basis for the continuation of research on mutually beneficial vectors of cooperation to combat the cybercrime of law enforcement bodies of Russia and Japan. The experience of performed research can underlie other options for interaction between different countries, including at the legislative level. Along with this, we are aware that the theses have polemical character regarding the proposed definitions and classification of cybercrime, due to the excessively rapid growth of tools and technologies in the hands of attackers. This study is the theoretical basis for the analysis of the practical experience of the crimes committed in several national laws of other countries for the subsequent refinement of the proposed classification of cybercrimes.

References

Al Azzam FAF (2019) The adequacy of the international cooperation means for combating cybercrime and ways to modernize IT. Janus.net 10(1): 66-83. doi: 10.26619/1647-7251.10.1.5

Borodkina TN, Pavlyuk AV (2018) Cybercrime: concept, content and countermeasures. Socio-political sciences 1:135-137

Broadhurst R and Chang L.Y.C. (2013) Cybercrime in Asia: Trends and Challenges. In: Liu J, Hebenton B, Jou S (eds.) Handbook of Asian Criminology. Springer, New York, NY. doi: https://doi.org/10.1007/978-1-4614-5218-8_4

Budapest Computer Crimes Convention (2001) Computer Information Crime Convention ETS N 185, Budapest, 23 November 2001. https://base.garant.ru/4089723/ Accessed 20 Apr 2020

Chernyakova AV (2018) International and foreign experience in criminal law counteraction to thefts committed using computer information. Jurisprudence and law enforcement practice 4(46):168-179

Christou G, Nitta Y (2018) EU-Japan cybersecurity cooperation. EU-Japan Security Cooperation: Trends and Prospects: 145-162. doi: 10.4324/9780429456114

Gady F-S (2017) Japan: The Reluctant Cyberpower. Asie.Visions, 91, IFRI, Marchhttps://www.ifri.org/sites/default/files/atoms/files/gady_japan_reluctant_cyberpower_2017.pdf Accessed 28 September 2017

Golovinov ON, Pogorelov AV (2016) Cybercrime in the modern economy: state and development trends. Issues of innovative economy 1: 73-88. doi: 10.18334/vinec.6.1.35353

Group-IB (2020) Website of the Group-IB. https://www.juniperresearch.com/home Accessed 20 Apr 2020

Juniper Research (2020) Website of the Juniper Research. https://www.juniperresearch.com/home Accessed 20 Apr 2020

Kallender P, Hughes CW (2017) Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. Journal of Strategic Studies 40 (1-2):118-145. doi: 10.1080/01402390.2016.1233493

Karpova DN (2014) Cybercrime: a global problem and its solution. Power 8: 46-50

Lakomov AS (2019) Cybercrime: modern trends. Academic thought 2(7):53-5.

Morozov NA (2014) Cybercriminality in Japan in the 21st century. Asian Pacific Region: economics, politics, law 3-4:100-109

Morozov NA (2014) The fight against computer crime in Japan. Society and Law 2(48): 141-145

Morozov NA (2016) Crime in modern Japan (problems of criminological and criminal law policies). Thesis 12.00.08 Criminal law and criminology; penal law. Moscow State University named after M.V. Lomonosov: 22. https://elibrary.ru/item.asp?id=30432469 Accessed 29 Apr 2020

Nomokonov VA, Tropina TL (2012) Cybercrime as a new criminal threat. Criminology: yesterday, today, tomorrow 24:45-55

Osipenko AL (2009) Network computer crime: theory and practice of struggle: monograph, 1st edn. (RF Ministry of Internal Affairs, Omsk Academy), 408 p.

Russian Federation Prosecutor General (2020) Website of the Russian Federation Prosecutor General. On crimes committed using modern information and communication technologies. https://genproc.gov.ru/smi/news/genproc/news-1431104/ Accessed 20 Apr 2020

Schjolberg S, Ghernaouti-Helie S (2011), A global treaty on cybersecurity and cybercrime, 2nd edn. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf Accessed 28 Apr 2020

Talipova LR (2016) International legal regulation of cybercrime. Humanitarian: socio-economic and social sciences 4:121-123

Valko DV (2016) Cybercrime in Russia and the world: a comparative assessment. Management in modern systems 3(10). URL: https://cyberleninka.ru/article/n/kiberprestupnost-v-rossii-i-mire-sopostavitelnaya-otsenka Accessed 22 Apr 2020

Zhuravlenko NI, Shvedova LE (2015) Problems of the fight against cybercrime and promising areas of international cooperation in this area. Society and Law 3(53):66-70