TRENDS AND METHODS OF FIGHTING CYBERCRIME IN THE RUSSIAN FEDERATION IN TERMS OF THE TRANSITION TO A DIGITAL ECONOMY*

AUTHORSHIP

Roman I. Dremliuga

Ph.D. in law, associate Professor, School of Law, Far Eastern Federal University, Vladivostok, Russia.

ORCID: https://orcid.org/0000-0003-1607-1228
E-mail: dreamluck@yandex.ru

Alexandr I. Korobeev

School of Law, Far Eastern Federal University, Vladivostok, Russia.

ORCID: https://orcid.org/0000-0003-2779-7809
E-mail: akorobeev@rambler.ru

Alexey Y. Mamychev

Doctor habil. in political science, Phd in legal science, head of the laboratory of political and legal research, Lomonosov Moscow State University, Professor of Vladivostok State University of Economics and Service.

ORCID: https://orcid.org/0000-0001-6528-2836
E-mail: mamychev@yandex.ru

Olga I. Miroshnichenko

School of Law, Far Eastern Federal University, Vladivostok, Russia, Ph.D. in Law, LI.M. In legal theory, Associate Professor of the Department of theory and history of state and law, Russia, Vladivostok, 8 Sukhanova Street.

ORCID: https://orcid.org/0000-0003-0135-3855
E-mail: olga-star.05@mail.ru

Received in:	**Approved in:**
2020-01-10	2020-01-29

DOI: https://doi.org/10.24115/S2446-6220202172701p.191-200

INTRODUCTION

Problem statement

We live in a time when cyberspace, as a part of a common information space, has become an important object of legal, political, economic, and social relations. Virtually every modern branch of science and technology uses digital technology and engineering. Therefore, since the beginning of 2000s, the theory has been gaining momentum and spread that by disrupting the operation of these networks, an entire state can be put out of action (BUDDKO, 2015). A number of incidents that became public, such as the massive attacks by hackers on large institutions and organizations around the world in 2017 (IRWIN, 2018), explain the relevance of studying cybercrime around the world.

President of the Russian Federation V.V. Putin, in his speech at the St. Petersburg International Economic Forum in 2017 (Vladimir Putin: Introduce digital technologies into all spheres of life // Official website of Rossiiskaia Gazeta, https://rg.ru/2017/06/04/reg-szfo/vladimir-putin-vnedrit-cifrovye-tehnologii-vo-vse-sfery-zhizni.html), emphasized the importance of developing the digital economy sector in Russia. The program for the development of the digital economy in any country in the world implies the introduction of new approaches in the regulation of public relations related to the circulation of computer information (IRWIN, 2018; LINKOV, 2018). That is why one of the main elements of the Russian state policy on the development of the digital economy is to ensure information security (Order of the Government of the Russian Federation of July 28, 2017, No. 1632-r "On approval of the "Digital economy of the Russian Federation" program), as the increase in the scale of "digitalization" of the economy entails increase in the role of protecting public and private information from criminal encroachments.

A BRIEF HISTORY OF FIGHTING CYBERCRIME

The Internet came to Russia much later than to North America and Europe - in 1994 and was primarily considered as a tool for an independent information space that would not lead to negative consequences. The emergence of the Internet in Russia coincided with the era of openness and the dismantling of the institutions that control the dissemination of information in society. The first regulations providing for criminal liability for computer crimes appeared in domestic legislation only with the adoption in 1996 of the Criminal Code of the Russian Federation and the introduction of Chapter 28 "Crimes in computer information". At the same time, computer crimes in our country were committed long before the entry into force of the Criminal Code of the Russian Federation. Probably the first well-known cybercrime in the USSR was the invasion of an automobile factory assembly line in 1983 (KONOVA, 1997).

* The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of research project n.18-29-16129.

Back then, the computer was just an object, means or instrument of various encroachments that could cover state and public security, crimes against personal and democratic rights, or crimes against property.

Summarizing Russian scientific research in cybercrime, we can conclude that the majority of Russian articles and monographs on this topic present it as a total and inevitable threat to the modern order, the only way to combat which is to limit and control cyber relations (GAPONENKO, 2015). At the same time, opinions are expressed why this is impossible: the speed of development of high technologies, the income they bring, and other positive aspects of virtualization make such restrictions utopian (SAVIOTTI, 2018).

After the enforcement of the Criminal Code of the Russian Federation, statistics reflected an extremely rapid growth in cybercrimes. If in 1997 only 30 of them were registered, then in 2000 there were already 760 (DREMLIUGA, 2008), and in 2017 - 1883, and the total number of crimes committed using information and telecommunication technologies in 2018 reached 90 thousand (The Prosecutor General's Office: the number of cyber frauds in the Russian Federation in 2018 increased by 7 times" Network edition "News. Economy", August 7, 2018). Most of the crimes (60-70%) were classified under Art. 272 of the Criminal Code of the Russian Federation. Crimes related to the creation, use, and distribution of computer viruses (Article 273 of the Criminal Code of the Russian Federation) ranked second (DREMLIUGA, 2008). Violations of the rules for the operation of computers (Art. 274 of the Criminal Code of the Russian Federation) accounted for the smallest share among the total number of registered computer crimes (DREMLIUGA, 2008).

At the same time, public opinion in the 90s and early 2000s did not recognize the danger behind cybercrimes. The concept of absolute freedom of dissemination of information that existed in society, limited only by the Criminal Code of the Russian Federation and industrial standards, low Internet penetration of the population and other factors led to a lack of control over the circulation of information on the Internet. Hackers were often recognized as genius people who, by accident or out of curiosity, violate the law, and their activities were not identified with crime, especially against the background of a sharp increase in violent crime inherent in Russia at that time (DREMLIUGA, 2014).

During that period, the average annual growth in murders was 20%, and the growth of all crimes was 13%, while the population growth was 0.4% (BADOV, 2009). Organized crime posed a real threat: more than one hundred and fifty criminal groups controlled up to forty thousand state enterprises and 90% of private enterprises (KUZNETSOVA, 1994; GAVRILOV, 2009). This led to the fact that law enforcement agencies threw their main resources not nearly into the fight against fledging cybercrime.

The situation changed only after 2010, when the legislator put up a serious barrier to the illegal dissemination of information. The obvious solution was to create a legal framework that obliged Internet providers to restrict access to such information. A special government body was created responsible for restrictions in cyberspace - the Federal Service for Supervision of Communications, Information Technology and Mass Media, also known as Roskomnadzor (http://roskomnadzor.ru), acting in accordance with the "Temporary regulations for the execution of the state function of creating, forming, and maintaining a unified automated system" ("Temporary regulations for the execution of the state function of creation, formation, and maintenance of "Unified Register of the domain names, website references and network addresses that allow identifying websites containing information circulation of which is forbidden in the Russian Federation" (approved by Roskomnadzor on 01.11.2012).).

In 2012, the Unified Register of the domain names, website references, and network addresses was developed and put into effect that allow identifying websites containing information circulation of which is forbidden in the Russian Federation (https://eais.rkn.gov.ru/faq/). It makes it possible, on the basis of a court decision, to add to this register the address of a site that distributes illegal content or information, and thereby carries out the so-called "filtering" of illegal content by hosting providers.

It is charged with storing personal data of Russian citizens who use the services of foreign companies on servers physically located in Russia. The purpose of the innovation was to

overcome the problem of jurisdiction over digital data belonging to Russian citizens. The new regime was introduced by Article 18 of Federal Law No. 152-FZ "On Personal Data" in 2014, which states: "When collecting personal data, for example, via the Internet, the operator must ensure the recording, systematization, accumulation, storage, clarification (updating, modification) and extraction of personal data of citizens of the Russian Federation through databases located on the territory of the Russian Federation.

CHARACTERISTICS OF CRIMINAL LEGISLATION

In 2017, the legislator amended the Criminal Code with Art. 2741 "Inappropriate influence on the critical information infrastructure of the Russian Federation". This article considered criminal "the creation, distribution, and/or use of computer programs or other computer information that are deliberately intended to improperly influence the critical information infrastructure of the Russian Federation, including for the destruction, blocking, modification, copying of information contained in it, or neutralization of means of protection of the specified information". Thus, Chapter 28 of the Criminal Code of the Russian Federation remains the main tool for combating crimes on the Internet. Chapter 28 of the Criminal Code of the Russian Federation criminalized the most dangerous types of encroachments on relations in the digital economy, in other words, computer relations. These include:

a) illegal access to computer information (Article 272 of the Criminal Code);

b) creation, use, and distribution of malicious computer programs (Article 273 of the Criminal Code);

c) violation of the rules for the operation of means of storage, processing, or transmission of computer information and information and telecommunication networks (Article 274 of the Criminal Code);

d) unlawful influence on the critical information infrastructure of the Russian Federation (Article 2741 of the Criminal Code).

That is, by no means all the acts which in literature mean crimes in cyberspace are included in the concept of "Crimes in computer information". They recognize only those acts that infringe on public relations regarding the security of computer information. According to the Budapest Computer Crime Convention of November 23, 2001, such crimes are categorized as "crimes against the confidentiality, integrity, and availability of computer data".

The object of the considered crimes is public relations in ensuring confidentiality, integrity, and availability of computer information; the safety and security of storage, processing and transmission of such information. The subject is computer information; means for storing, processing or transmitting computer information; information and telecommunication networks; and terminal equipment. The concept of "computer information" is disclosed in note 1 to Article 272 of the Criminal Code. It means information (messages, data) presented in the form of electrical signals, regardless of the means of their storage, processing, and transmission.

The means of storing, processing, and transmitting computer information themselves are material carriers, regardless of the prevalence of their use. This includes floppy discs, hard drives, optical discs, memory cards, flash cards, external hard drives, etc. The tool for processing computer information is an electronic device designed for its automatic processing by performing tasks determined by a sequence of operations. In other words, a computer, not only a PC, but also everything that processes digital information (phone, camera, tablet, etc.), as well as an analog device (for example, an airplane autopilot).

The objective side of acts committed in computer information can be expressed in the form of both actions (Articles 272, 273 of the Criminal Code) and inaction (Articles 274, 274[1] of the

Criminal Code). All structures (except for the acts provided for in Part 1 of Art. 273 and Part 1 of Art. 274[1] of the Criminal Code) are material, and the consequences in the main elements of computer crimes are the destruction, blocking, modification, copying of computer information, major damage, and harm.

Destruction of computer information means making it completely unusable for its functional purpose (for example, erasing it from a hard disk). Blocking information involves creating obstacles to free access to information while preserving the information itself. Modification of information is the introduction of any changes to the original information without the consent of the copyright holder. Copying information means its reproduction in any material form.

In terms of subjective aspect, the creation, use and distribution of malicious computer programs (Article 273 of the Criminal Code), as well as illegal influence on the critical information structure of the Russian Federation (parts 1 and 2 of Article 2741 of the Criminal Code) suggests only a deliberate form of guilt. The rest of the computer crimes can be both intentional and negligent.

The subject of crimes under Articles 272, 273 CC, is a person aged 16 and older. The subject of the crime under Article 274 of the Criminal Code is special. It can only be a person who is entrusted with the obligation to comply with the rules for the operation of storage, processing, transmission of computer information, information and telecommunication networks or terminal equipment.

Qualified and *especially qualified* types of computer crimes are the same acts committed out of selfish interest, by a group of persons by prior conspiracy, by an organized group, by a person using his official position, causing or threatening with severe consequences.

Note that since the introduction of an independent Chapter 28 "Crimes in computer information" into the Criminal Code of the Russian Federation, the problem of outdated terminology has remained quite serious. It was only on December 7, 2011, that the term "electronic computer" was excluded from all the norms included in the chapter, which significantly increased the scope of application of the relevant norms. Their version has also changed significantly. Art. 272 of the Criminal Code introduced a note revealing the concept of computer information, and in 2017 the chapter was supplemented with a new Article 2741 (Inappropriate influence on the critical information infrastructure of the Russian Federation) of the Criminal Code of the Russian Federation.

At the same time, the innovation gave rise to a number of new, legal problems. Their reason lies in the fact that any signals are directly related to information carriers and means of their storage. Thus, they can be electrical, electromagnetic, optical, etc. The Criminal Code of the Russian Federation, however, deals exclusively with electrical signals. Meanwhile, information is converted into an electrical signal only at the time of processing and its final transmission. In this regard, in the theory of criminal law, there is a proposal to clarify the wording, calling the electrical signal "final", i.e. already entered into the computing device.

Judicial practice is faced with another problem when applying Article 273 of the Criminal Code. The previous version of this rule provided only such malicious programs that could obviously lead to criminal consequences. The criminal law has fought against illegal activities of a fairly limited circle of people (hackers, computer fraudsters, etc.).

New version of Article 273 of the Criminal Code allows expanding the applicability of the norm to almost any user of unlicensed software. The article in its current form equated with malicious computer programs those that are designed to neutralize the means of protecting computer information (GAVRILOV, 2009). All so-called “patches”, “keygens”, “cracks” and similar software can now be considered malware (INOGAMOVA-KHEGAY, 2018). As a result, both the creators and distributors of "warez" software (which was the case before) and ordinary users, which are representatives of most of the Russian computer community, can be charged with a criminal offence under Article 273 of the Criminal Code.

In accordance with the provisions of the resolution of the Plenum of the Supreme Court of the Russian Federation of April 26, 2007 "On the practice of consideration by courts of criminal cases on violations of copyright, related, inventive and patent rights, as well as on illegal use of a trademark" by dealers (distributors) of malicious software in the form of "unregistered

software" will be considered persons assisting in its distribution, for example, by placing a hyperlink to a resource where the file is physically stored. Considering the practice developed in law enforcement agencies, identifying the person who posts the link to the "hacked software" and bringing him to criminal responsibility will have little difficulty (BATURIN, 2011).

One of the problematic issues in the process of qualifying computer crimes is their delimitation from related criminal acts. In particular, the question arises, whether it is legitimate to qualify the pirated replication of computer programs only under Article 146 of the Criminal Code, and the theft of funds using computer networks - only under Articles 158 and 159 of the Criminal Code. Or, in these cases, additional qualifications are also required under the articles on responsibility for computer crimes?Scientists have split over. Some of them believe that the computer in such situations is only a means of committing crimes, and therefore qualification by aggregate cannot take place (TROPINA, 2009). Others insist on the need for additional imputation of computer crimes (LYAPUNOV, 2009).

The above situations seem to be an ideal combination of crimes. When non-cash money is stolen using a computer through unlawful access to legally protected computer information with subsequent modification or copying of this information, the attacker not only infringes on property relations but also harms another group of public relations related to ensuring the confidentiality of protected computer information. As a result, we have an ideal combination of crimes against property (Articles 158 and 159 of the Criminal Code) and in computer information (Article 272 of the Criminal Code). A similar set can be found in the case of copyright infringement by selling counterfeit copies of works obtained in the process of illegal access to protected computer information.

NEW CHALLENGES

A serious challenge is the widespread use of artificial intelligence systems - computer systems or programs that imitate one or more aspects of intellectual behavior, which have a higher degree of self-determination (autonomy) and independence from the will of the developer or user compared to other computer systems or programs. Some intelligent systems are capable of learning and self-learning.

Already, such systems can be actively used to identify the weaknesses of potential victims of fraud, as well as to imitate human activities. Here are some small examples. One of the intelligent systems can, with a high degree of reliability, establish sexual orientation from a photograph of a person posted on social networks (New AI can guess whether you're gay or straight from a photograph <https://www.theguardian.com/technology/2017/sep/07/new-artificial-intelligence-can-tell-whether-youre-gay-or-straight-from-a-photograph>(last accessed February 5, 2018). The other is capable of recognizing political beliefs and intelligence (Face- reading AI will be able to detect your politics and IQ, professor says <https://www.theguardian.com/technology/2017/sep/12/artificial-intelligence-face-recognition-michal-kosinski> (last accessed February 5, 2018)). Such systems can be used to manipulate the will of the voter in elections (CHEN ET AL., 2017) and their use poses a significant social threat.

There are intelligent systems that simulate a person's voice (https://lyrebird.ai/; https://www.technologyreview.com/the-download/610386/a-new-algorithm-can-mimic-your-voice-with-just-snippets-of-audio/) or video image (https://www.fakeapp.org/; https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html). They create audio and video recordings to manipulate people. That is, artificial intelligence systems are not just another computer tool for committing crimes. They threaten the entire existing public order, provoking an "information apocalypse" (Stover, 2018), in which fact becomes indistinguishable from fiction, and people stop trying to understand the difference. This undermines confidence in any information and can destabilize society.

In general, we can conclude that modern Russian legal science has several theories established regarding the social danger of cybercrime. The first theory concerns the crime of cyberterrorism and its relationship with the general level of manifestation of extremism and terrorism both in Russia and around the world. Scientists note that modern advances in

scientific and technological progress increase the likelihood of using initially peaceful technologies as a means of conducting cyberattacks, and the creators of technologies sometimes don't even realize such use to their detriment (SOLODOV, 2018).

Views have been expressed that the increase in the sophistication of cyber terrorist acts is due to the fact that today cyber terrorists have a real opportunity to disrupt the normal functioning of critical state facilities (nuclear reactors, biological and chemical laboratories and other similar objects), which will entail an innumerable number of victims (SOLODOV, 2018). Still, the main forms of cybercrime are insult, defamation, and harassment (Hamby, 2018), followed by fraud (BATAEVA, 2016), blackmail and extortion, theft of funds, etc. (REEP-VAN DEN BERGH, 2018), and anarchist groups on the Internet, the so-called "Shadow Internet", are focused on the fight against intellectual property rights and censorship in general, rather than on hate crimes. Therefore, it is not always correct to mix cybercriminals and terrorists who use Internet power to propagandize and involve persons in real terrorist crimes, and do not agree with the identification of signs indicating an improvement in the technical equipment of cyberterrorists, and the separation of cyberterrorism as a "technological type of terrorism" (CULLEN, 2017).

Another theory is to highlight the tendency for cybercrime to become a long-term factor in the political and economic process. According to its adherents, this is due to the lack of major successes in countering cybercrime over the past decade, the formation of new prerequisites for its further spread (DEMIANOVA, 2018; KOMLEV, 2018). Some researchers argue with this theory that the internetization of the population leads to a decrease in negative social activity, translating it into so-called "network wars" that have no real victims, or allowing people who are unable to improve their financial situation due to various social economic reasons, find remote work via the Internet, get financial support for their projects, improve the level of education through online training platforms, etc. (KISILEVA, 2018; KARABANOVA, 2012).

Similar points of view existed when additional elements of crimes of incitement to suicide were introduced into the Criminal Code of the Russian Federation (Articles 1101 and 1102 of the Criminal Code of the Russian Federation), where the Internet and cyber technologies are among the means and methods of committing. Their authors noted, referring to statistics, that the ratio of suicides is inversely proportional to the spread of the Internet, since it is easier for a person to find support, communication of interests, psychological, social, financial and even legal assistance in the virtual space due to the absence of physical restrictions and the availability of information (DIUMAEVA).

We would also like to note that the steady trend towards the distinguishing cybercrime as a separate form is in fact an evolution of existing crimes, namely the methods and means of their commission. Thus, in Russia, the erroneous qualification of such a crime as a violation of the inviolability of private life (Article 137 of the Criminal Code of the Russian Federation) under Article 272 of the Criminal Code of the Russian Federation (Illegal access to computer information), if the crime was committed using cyber technologies, or, more simply, through access to e-mail, social networks, instant messengers, etc. The reason, in our opinion, lies in the excessive criminalization of additional methods of committing crimes, or even entire compositions which indicate computer information, digital technologies, the Internet, etc. on the objective side. In addition, such technologies are often perceived by the legislator on a one-dimensional basis, without considering their originality and almost complete regulation by the current law due to the information basis of existence. An example of such relations can be not only computer information as such, but also cryptocurrency, unmanned aerial systems, blockchain, cloud technologies, virtual reality (DREMLIUGA, 2019; DREMLIUGA, IAKOVENKO, 2019).

SUMMARY

In other words, at this stage of the development of law and its attempts to correspond to the transition of the world community to the era of digital technologies, science and practice increasingly face an erroneous perception of digital reality. For example, in the case of assessing the public danger of cyber terrorism, cybercrime, cyber espionage and terrorism are

often mixed into one type of criminal activity. Whereas, in our opinion, this point of view is dangerous and even destructive for legal and law enforcement activities, since it leads to the creation of conspiracy theories about a non-existent form of criminal organizations.

Extremism on the Internet also seems to the legislator to be excessively socially dangerous, as its commission via the Internet, according to the legislator, aggravates the public danger of the act by virtue of practically unlimited public access to a publication or speech. We, without disputing the significance of the object of these crimes, nevertheless consider a different point of view expressed, for example, by M.I. Khalikov. He quite rightly asserts that the ideological component is important for separating extremism from other crimes, since "a certain ideology is the motivation for extremism as an activity" (KHALIKOV, 2008).

Here, as with a number of other crimes, there is a serious misconception. Just as a hooligan motive is often misrepresented as a motive of political, religious, national, racial, and other hatred or enmity, or as a motive of hatred or enmity in relation to any social group, other structures ("classic" for criminal laws not only in Russia, but also foreign states) often acquire "doubles" in the form of avatar norms, highly imperfect in terms of the theory of criminal law prohibition. Then deliberate harm or destruction of someone else's property is criminalized in relation to computer information as unlawful access, which entailed its destruction, and fraud receives a "duplicate clone" in the form of fraud in the field of computer information (Article 159.6. of the Criminal Code of the Russian Federation), essentially representing a declaration punishable by a separate method of committing this crime. This legislative practice leads to the fact that such an article becomes casual, that is, requiring an explanation of its meaning for each specific case. The lack of proper interpretation can lead to both an unlawful refusal to initiate a criminal case, and to the prosecution of a person whose actions do not contain corpus delicti, or they have committed another act prohibited by the Criminal Code of the Russian Federation.

Summing up, we note that the Russian Federation has recognized cybercrime as the main threat to state security and the stability of society. This is reflected both in the development of criminal-legal measures to combat cybercrimes and in preventive measures of an administrative nature. Objects of the so-called critical information infrastructure received special legal protection. The article also reviewed the social danger of some cybercrimes having been already liable to criminal responsibility. According to the legislator, the use of the Internet aggravates the social danger of the act.

ACKNOWLEDGMENTS

The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of research project No. 18-29-16129

REFERENCES

BADOV, A.D. Geography of crime in Russia: Changes during the post-soviet period. *Vestnik Moskovskogo Universiteta, Seriya 5: Geografiya*, *2*, 61-65, 2009.

BATAEVA, T.A. Actual problems of struggle against fraud in the sphere of computer information. *Collection of articles of the international scientific-practical conference "Science in modern society: regularities and development tendencies": in 2 parts,* 143-145. (In Russian). 2016.

BATURIN, YU.M., ZHODZINSKIY, A.M. Computer criminality and computer safety. M., C. 135. (In Russian). 2011.

BUDDKO, M.V. Cybercrime as a threat to the world economy generated by informatization. *Economy and society, 2-1*(15), 776-779. (In Russian), 2015.

CHEN, J., FALISZEWSKI, P., NIEDERMEIER, R., TALMON, N. Elections with few voters: Candidate control can be easy. *Journal of Artificial Intelligence Research*, *60*, 937-1002, 2017.

CULLEN, F. T. (ED.). Technology and terrorism. Routledge. 244 p, 2017.

DEMIANOVA, T.A., POTIENKO, P.A. Cybercrime as a threat to the modern society security. *Vestnik of the Moscow Institute of Public Administration and Law*, *2*(22), 12-14. (in Russian) 2018.

DREMLIUGA, R. Crimes in Virtual Reality. *Revista Dilemas Contemporáneos: Educación, Política y Valores, 7*(1), 1-14, 2019. https://dilemascontemporaneoseducacionpoliticayvalores.com/_files/200006019-371bb371bc/19.09.129%20Delitos%20en%20realidad%20virtual.pdf

DREMLIUGA, R. *Internet Crime*. Published in Russian by the Far Eastern National University Press, 240 p. (in Russian), 2008.

DREMLIUGA, R. Subculture of hackers in Russia. *Asian Social Science*, *10*(18), 158-162, 2014.DOI: 10.5539/ass.v10n18p158

DREMLIUGA, R., IAKOVENKO, A., PRISEKINA, N. Crime in virtual reality: Discussion. *International Conference on Cybersecurity 2019* (*ICoCSec 2019)*, 8970947. 81-85, 2019.

GAPONENKO, V.F., TAIGILDIN, D.V. Maintenance of economic security of the state by counteraction to economic crimes in system of modern information technologies. *Mechanism of economic-legal maintenance of national security: experience, problems, prospects Proceedings Materials of VIII International scientific-practical conference*, 9-11, 2015. (in Russian)

GAVRILOV, V.M. Counteraction of crimes committed in the sphere of computer and mobile communications by the organized criminal groups. Saratov, 248 p. (in Russian), 2009.

HAMBY, S. ET AL. Digital poly-victimization: The increasing importance of online crime and harassment to the burden of victimization. *Journal of Trauma & Dissociation*, *19*(3), 381-386, 2018.

INOGAMOVA-KHEGAY, L.V., KIBALNIK, A.G., KLENOVA, T.V., KOROBEEV, A.I., LOPASHENKO, N.A. Actual problems of criminal law. Part Special: textbook for masters. Moskow. 340 p, 2018 (in Russian)

IRWIN, A.S.M. Double-Edged Sword: Dual-Purpose Cyber Security Methods. *Cyber Weaponry*. Springer, Cham, 101-102, 2018.

KARABANOVA, N.M. Stress-management: "price" of stress. *Proceedings of scientific-practical conference "Management in social-ecological systems"*. Published in Vladimir, 642-646, 2012 (in Russian)

KHALIKOV, M.I. Extremism (criminal legal aspect). *Vestnik of Udmurtia University*. *Economics and law series*, *2-2,* 208-215, 2008 (In Russian)

KISELEVA, S.O. As a young specialist to find a good job. *Collection of scientific papers "Actual problems of socio-ecological culture"*. Published in Ufa, 125-131, 2018. (in Russian)

KOMLEV, YU.YU. Deviance and criminality in the epoch of high technology, consumerism and glam capitalism. *MVD Vestnik of Kazan legal institute*, *1*(31), 23-34, 2018 (in Russian).

KONOVA, E.N. Modern problems of struggle with computer crimes. *Izvestia vysokhraneniya. Jurisprudence, 2,* 157-161, 1997 (in Russian)

KUZNETSOVA, N.F. Crime in Russia: Causes and Prevention. Demokratizatsiya (Journal of Post Soviet Democratization), 1994, 443; Gavrilov V.M. Counteracting crimes in computer and mobile communications committed by organized crime syndicates. Saratov, 22-28, 2009.

LINKOV, I., TRUMP, B.D., POINSATTE-JONES, K. Governance strategies for a sustainable digital world. *Sustainability (Switzerland)*, *10*(2), 440, 2018. Access at: http://www.mdpi.com/2071-1050/10/2/440/htm.

LYAPUNOV, YU., MAXIMOV, V. Responsibility for the computer crimes. *Legitimacy, 1,* 15-26, 2009. (in Russian)

REEP-VAN DEN BERGH, C. M.M., JUNGER, M. Victims of cybercrime in Europe: a review of victim surveys. *Crime science, 7*(1), 1-17, 2018.

ROMAN, D. Research of public accessibility of the drug promotion information in the Russian-language internet. *Mediterranean Journal of Social Sciences, 6*(3), 540-543, 2015. DOI: 10.5901/mjss.2015.v6n3s1p540

Russian Federation Government Decree of 28.07.2017 n. 1632-r "On Approval of the program "Digital Economy of the Russian Federation". "*Collection of Legislation of the Russian Federation*", 07.08.2017, n. 32, Art. 5138.

SAVIOTTI, P.P., METCALFE, J.S. Present development and trends in evolutionary economics. *Evolutionary theories of economic and technological change. – Routledge,* c. 1-30, 2018.

SOLODOV, A. ET AL. Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities. *Security Journal*, *31*(1), 306-310, 2018.

STOVER, D. Garlin Gilchrist: Fighting fake news and the information apocalypse. *Bulletin of the Atomic Scientists*, *74*(4), 283-288, 2018.

TROPINA, T.L. *Cybercrime. Concept, state, criminal-legal measures of struggle.* Vladivostok. 235 p, 2009 (In Russian)

Trends and methods of fighting cybercrime in the Russian Federation in terms of the transition to a digital economy

Tendências e métodos de combate ao crime cibernético na Federação Russa em termos de transição para uma economia digital

Tendencias y métodos de lucha contra la ciberdelincuencia en la Federación de Rusia en términos de la transición a una economía digital

Resumo

O artigo trata do problema do combate ao cibercrime na Federação Russa no contexto de sua transição para a economia digital. A sociedade e o estado nos anos 90 e no início dos anos 2000 não reconheciam o perigo por trás dos crimes cibernéticos. O conceito de liberdade absoluta de divulgação de informações, que existia na época, e outros fatores levaram a um grande aumento do crime cibernético hoje. Os autores concluíram que a situação mudou apenas na última década, quando começaram a lutar contra o crime cibernético de forma abrangente. O artigo também discute a questão da delimitação de crimes cibernéticos de atos criminosos relacionados. A Federação Russa reconheceu o cibercrime como a principal ameaça à segurança do Estado e à estabilidade da sociedade. Isso se reflete tanto no desenvolvimento de medidas jurídico-criminais de combate aos crimes cibernéticos, como em medidas preventivas de natureza administrativa. Os objetos da chamada infraestrutura crítica de informação receberam proteção jurídica especial. O artigo também analisou o perigo social de alguns crimes cibernéticos já estarem sujeitos à responsabilidade criminal.

Palavras-chave: Combate ao crime cibernético. Federação Russa. Economia digital.

Abstract

The article deals with the problem of combating cybercrime in the Russian Federation in the context of its transition to the digital economy. Society and the state in the 90s and early 2000s did not recognize the danger behind cybercrimes. The concept of absolute freedom of dissemination of information, which existed at the time, and other factors have led to a high increase in cybercrime today. The authors concluded that the situation changed only in the last decade, when they began to fight against cybercrime in a comprehensive manner. The article also discusses the issue of delimiting cybercrimes from related criminal acts. The Russian Federation has recognized cybercrime as the main threat to state security and the stability of society. This is reflected both in the development of criminal-legal measures to combat cybercrimes and in preventive measures of an administrative nature. Objects of the so-called critical information infrastructure received special legal protection. The article also reviewed the social danger of some cybercrimes having been already liable to criminal responsibility.

Keywords: Fighting cybercrime. Russian Federation. Digital economy.

Resumen

El artículo aborda el problema de la lucha contra el ciberdelito en la Federación de Rusia en el contexto de su transición a la economía digital. La sociedad y el estado en los años 90 y principios de los 2000 no reconocieron el peligro detrás de los delitos cibernéticos. El concepto de absoluta libertad de difusión de información, que existía en ese momento, y otros factores han llevado a un alto aumento de la ciberdelincuencia en la actualidad. Los autores concluyeron que la situación cambió solo en la última década, cuando comenzaron a luchar contra el ciberdelito de manera integral. El artículo también analiza la cuestión de delimitar los delitos cibernéticos de los actos delictivos relacionados. La Federación de Rusia ha reconocido que el delito cibernético es la principal amenaza para la seguridad del Estado y la estabilidad de la sociedad. Esto se refleja tanto en el desarrollo de medidas penales-legales para combatir los delitos cibernéticos como en las medidas preventivas de carácter administrativo. Los objetos de la denominada infraestructura de información crítica recibieron protección jurídica especial. El artículo también revisó el peligro social de que algunos ciberdelitos ya estén sujetos a responsabilidad penal.

Palabras-clave: Lucha contra la ciberdelincuencia. Federación Rusa. Economía digital.