Cybercrime and Digital Transformation

Viktor P. Kirilenko
Doctor of Sciences (Jurisprudence), Professor, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Sankt Petersburg, Russian Federation; kirilenko-vp@ranepa.ru
Georgy V. Alekseev
PhD in Jurisprudence, Associate Professor, North-West Institute of Management, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Sankt Petersburg, Russian Federation; deltafox1@yandex.ru

ABSTRACT
Cyberspace crime is a critical threat to the information security of the state and civil society institutions. Inside global network the abuse of computer user's trust allows organized criminal groups to achieve their economic and political goals by committing offenses in the international information space. The methods of participatory observation, comparative legal and discourse analysis show that digital transformation has weakened the influence of the state on the development of the cultural sphere of society, and computer technologies have become the object of interests of criminal structures. Digital transformation has created virtual reality based on the laws and regulations of the networked community. Civil society by rejecting most of the peremptory norms imposed by national governments for political purposes produce victims of a wide range of cybercrimes: fraud and computer misuse offences and obscene publications. Since digital transformation is a universal phenomenon that will inevitably change the life of the entire world community, it is necessary to reach a consensus on the development and implementation of modern international agreement which, on the one hand, will guarantee freedom of speech and the right of every person to access information, and on the other hand will protect citizens, states and social institutions from criminal encroachments in an actively developing digital environment.
Keywords: human rights, crime, information, fraud, extremism, hacker, responsibility, public danger, technology

The Secretary-General of the United Nations, Antonio Guterres, in November 2018, commenting on the work of the United Nations Office on Drugs and Crime (UNODC), drew attention to the fact that «new technologies, including big data, artificial intelligence and automation, are entering an era of transformation, ...and, despite the benefits that such progress brings, it also contributes to the emergence of new forms of crime»[1]. It is obvious that the development of information technologies, creating a virtual environment for public relations, actualized new criminal schemes with unique and insufficiently studied ways of committing crimes (modus operandi). In the context of digital transformation, when questions arise about the responsibility for decisions made by artificial intelligence, and the machine processing of big data almost completely eliminates the possibility of regulatory restrictions on access to information for a long time, the legislator is faced with the task of creating such criminal law norms that will simultaneously promote technological progress and bring to justice those responsible for committing crimes.

The development of national legislation in the context of digital transformation lags behind the pace of technological progress. Artificial intelligence, various elements of which are systematically developed and implemented by transnational corporations, is designed to promote the achievement of sustainable development goals[2], and the response of the state apparatus to the formation of a cross-border and self-developing cybernetic environment is predetermined by the interest of social institutions in organizing international dialogue on the scale of the global media space. It is obvious that global systems of international communication do not give individuals the right to abuse freedom of speech[3], to use artificial intelligence and big data for criminal purposes[4], to create criminal communities in the virtual space[5]. However, the differences in the understanding of the legitimacy of various forms of protest behavior raise the issue of the difference in the cyberspace of the

[1] «Much work to do and no time to waste» in cybercrime fight, says UN chief [Online source]. URL: https://news.un.org/en/story/2018/05/1009692 (date of access: 25.02.2021)
[2] See: Tomasevic V., Ilic-Kosanovic T., Ilic D. (2020) Skills Engineering in Sustainable Counter Defense Against Cyber Extremism. In: Al-Masri A., Al-Assaf Y. (eds) Sustainable Development and Social Responsibility. Vol. 2. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham. D0I:10.1007/978-3-030-32902-0_25
[3] Kirilenko, V. P., Shamakhov, V. A., Alekseev G. V. Freedom of Speech and Media Safety [Svoboda slova i mediabezopasnost']. SZIU RANEPA. St. Petersburg. 2019. 440 p. (in Russian)
[4] Begishev, I. R. Khisamova, Z. I. Criminological Risks of Using Artificial Intelligence [Kriminologicheskie riski primeneniya iskusstvennogo intellekta] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 767-775. DOI: 10.17150 / 2500-4255.2018.12 (6). 767-775. (in Russian)
[5] See.: Broadhurst R. G., P. Grabosky, M. Alazab, S. Chon. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime // International Journal of Cyber Criminology. 2014. Vol. 8. Iss. 1. Pp. 1-20. DOI: 10.2139/ssrn.2345525

actions of modern criminals and «partisans» who want to «stay in the political sphere» and do not want to «fall into the criminal sphere» in their desire to force a change in the order of life[6].

Vice-President of the European Commission MargaritisSchinas at the meeting of the Commission on January 29, 2020 emphasized that «the fight against cybercrime is a key part of the work to create a European Union that protects its citizens. Cybercriminals know no boundaries.»[7] At the same time, the broad international recognition of the threats and dangers of criminal activity in the virtual space of computer networks has not brought the world community closer to a consensus in distinguishing between legitimate democratic protest and criminal propaganda of violent extremism. Statistics on cybercrime show that, while about 80% of criminals in the virtual space commit offenses from selfish motives[8], the rest of the attackers express their behavior in active protest against the political system and modern civil ethics.

The nature of the impact of digital transformation on the dynamics of cybercrime is determined by the rationality of the use of computer technologies, thanks to which new objects of legal regulation appear, such as social networks, virtual things and multimedia information resources. With the expansion of the possibilities of digital technologies, all spheres of society are being transformed, which means that the criminal world is also changing, where there is less gross violence and more high technologies appear. As the anonymity of Internet users and their physical distance from each other contribute to the prosperity of fraud in the virtual world, the level of trust in Internet resources also decreases. Given the low level of mutual trust and disunity of social media users, criminal communities that rely on radicalization and violent extremism in the virtual space, as a rule, have little chance of success. The agenda of multimedia information resources is dictated by digital multinational corporations, which are not interested in criminalizing their own business and act as natural allies of law enforcement agencies in countering various manifestations of violent extremism.

American scientist Sidney Tarrow describes any active protest as «power in motion», where the inspiration of the protesters who have experienced social stigma, police dogs, rubber bullets, fights and even the death of friends arises when people come together to collectively realize their aspirations[9]. When using the virtual space of the Internet to express political protest, many activists and researchers of social movements are skeptical about the potential consequences of Internet activism, preferring offline protest as a «real protest»[10]. However, the low effectiveness of virtual protest does not exclude the efforts of extremist communities to radicalize public opinion through «online protest»[11] with the subsequent escalation of radicalization to the level of «real protest»[12].

It is obvious that a broader implementation of Federal Law No. 436-FZ of December 29, 2010 «On the protection of children from information harmful to their health and moral development»[13] and a number of relevant legal norms can serve as a legal means of protecting minors from certain manifestations of cybercrime. At the same time, the expertise of information products, firstly, depends on the qualifications of experts and their moral and political views, and secondly, is limited to the legal space of Russia. According to the reasoned opinion of Professor A. I. Bastrykin, «the responsibility for the safety of the child when he communicates on the Internet should be taken by his family. After all, unlike direct contact with a criminal, it should be easier for a child to stop communicating with a pedophile on social networks.»[14]

The virtual world of social networks and the interface of computer programs differ significantly from real actions and direct communication, since the logic of the virtual act and its consequences depend on the features of the digital environment within which communication takes place and legally significant actions are performed. In the virtual space, deliberately low-

---

6 Kirilenko, V. P., Alekseev, G. V. The Legitimacy of Democracy in the Works of Max Weber and Karl Schmitt [Legitimnost' demokratii v rabotakh Maksa Vebera i Karla Shmitta] // Jurisprudence [Pravovedenie]. 2018. Vol. 62. No. 3. Pp. 501-517. DOI: 10.21638/11701/spbu25.2018.305. (in Russian) P.511 See also: Schmitt Carl. Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen. Duncker & Humblot. 1963.

7 Cybercrime: New Survey Shows Europeans Feel Better Informed but Remain Concerned [Online source]. URL: https://ec.europa.eu/commission/presscorner/detail/hr/ip_20_143 (date of access: 01.03.202)

8 Kirilenko, V. P., Alekseev, G. V. Harmonization of Russian Criminal Legislation on Combating Cybercrime with the Legal Standards of the Council of Europe [Garmonizatsiya rossiiskogo ugolovnogo zakonodatel'stva o protivodeistvii kiberprestupnosti s pravovymi standartami Soveta Evropy] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2020. Vol. 14. No. 6. Pp. 898-913. DOI: 10.17150/2500-4255.2020.14(6).898-913. (in Russian)

9 Tarrow S. Power in Movement: Social Movements, Collective Action and Politics. New York: Cambridge University Press. 1994. 251 p

10 See: Rucht D. Movement Allies, Adversaries, and Third Parties. 2007. DOI:10.1002/9780470999103.ch9

11 See: Ammar J. Cyber Gremlin: Social Networking, Machine Learning and the Global War on Al-Qaida and IS-inspired Terrorism // International Journal of Law and Information Technology. 2019. Vol. 27, iss. 3. Pp. 238-265. DOI: 10.1093/ijlit/eaz006; Awan I. Cyber-extremism: Isis and the Power of Social Media // Social Science and Public Policy 2017. Vol. 54. Pp. 138-149. DOI: 10.1007/s12115-017-0114-0; Earl J. Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M. Giugni & K. Uba (Eds.). The Consequences of Social Movements. Cambridge: Cambridge University Press. 2016. Pp. 363-400. DOI: 10.1017/CBO9781316337790.015

12 Supra note 10

13 Odintsova, N. E., Repetskaya, A. L. Problematic Aspects of Domestic and Foreign Legislation in Countering the Propaganda of Pedophilia [Problemnye aspekty otechestvennogo i zarubezhnogo zakonodatel'stva v protivodeistvii propagande pedofilii] // International Journal of Humanities and Natural Sciences [Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk]. 2019. No. 11-3 (38). Pp. 84-89. DOI: 10.24411/2500-1000-2019-11821. (in Russian)

14 Bastrykin, A. I. Crimes Against Minors in the Internet Space: On the Issue of Victimological Prevention and Criminal- Legal Assessment [Prestupleniya protiv nesovershennoletnikh v internet-prostranstve: k voprosu o viktimologicheskoi profilaktike i ugolovno-pravovoi otsenke] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2017. Vol. 11. No. 1. Pp. 5-12. DOI: 10.17150/2500-4255.2017.11 (1).5-12. (in Russian)

quality and counterfeit goods are sold, Darkweb resources allow you to organize trade in goods withdrawn from economic circulation and pay for services of openly criminal content[15], extremist communities recruit supporters through social networks[16]. Online extremism, aimed at radicalizing public opinion and recruiting new supporters, is carried out by organized criminal groups[17]. Studies in the field of media security[18] and violent extremism[19] demonstrate the irrationality of the media logic of propaganda of violent extremism, which is partly due to the interest of radical groups in recruiting individuals suffering from mental disorders, including murder-suicide syndrome[20].

The digital transformation has changed the perception of crime so much that it is sometimes difficult to distinguish victims from accomplices in crime, and the methodology for scientific assessment of the dynamics of cybercrime predicts an increase in online crime[21]. A review of available victimization surveys shows that between 2010 and 2020, cybercrime can account for between one-third and one-half of crimes in developed countries[22]. In Russia before the easing of the criminal policy in 2018 in relation to extremist offenses in the virtual space, the number of crimes of a terrorist nature and extremist orientation grew rapidly[23]. There is every reason to believe that the increase in computer crime has contributed to a decrease in the level of traditional crime, and cybercrimes themselves are not included in the official statistics. While the degree of public danger of cybercrime is steadily increasing, it is clear that «the largest part of cybercrime remains outside the scope of statistics».[24]

The harmonization of the Russian criminal legislation in the field of digital technologies with the norms of the criminal law of developed countries is a necessary condition for the organization of international police cooperation. The need for international cooperation in countering cybercrime is determined by the absence of state borders in the information space. The development, under the auspices of the Council of Europe, of the Convention on Cybercrime ETS No. 185 (Budapest, 23 November 2001) and the ratification of this agreement by the majority of the Council of Europe member States is an important element of global cybersecurity. The Additional Protocol to the Convention on Cybercrime concerning the criminalization of offences related to manifestations of racism and xenophobia committed through Computer Systems, ETS No. 189 (Strasbourg, 28 January 2003), extended the Convention to extremist offences.

The Russian Federation is not a party to the Convention on Cybercrime, but most of the provisions of the Budapest Convention have become widely accepted norms of customary international law. Despite the fact that the Order of the President of the Russian Federation of March 22, 2008 No. 144-rp was canceled by the order of the President of the Russian Federation of November 15, 2005. No. 557-rp «On signing the Convention on Cybercrime»[25], the rationality of most of the provisions of this Convention is not in doubt, since it was initially emphasized that «the Russian Federation proceeds from the fact that the provisions of paragraph «b» of article 32 of the Convention are formulated in such a way that they can harm the sovereignty and national security of the participating States, the rights and legitimate interests of their citizens and legal

---

15 See: Martin J., Munksgaard R., Coomber R. & oths. Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards // British Journal of Criminology. 2020. Vol. 60, iss. 3. Pp. 559-578. DOI: 10.1093/ bjc/azz075

16 See: Earl J. Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M. Giugni & K. Uba (Eds.). The Consequences of Social Movements. Cambridge: Cambridge University Press. 2016. Pp. 363-400. DOI: 10.1017/CBO9781316337790.015; Taylor R. W. Fritsch E. J., Liederbach J. Digital Crime and Digital Terrorism. New York: Prentice Hall Press, 2014. 416 p

17 Broadhurst R. G., P. Grabosky, M. Alazab, S. Chon. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime // International Journal of Cyber Criminology. 2014. Vol. 8, iss. 1. P. 1-20. DOI: 10.2139/ssrn.2345525; Dalgaard-Nielsen A. Violent Radicalization in Europe: What We Know and What We Do Not Know // Stud Conflict Terrorism 2010. Vol. 33, iss. 9. P. 797-814. DOI: 10.1080/1057610X.2010.501423; Walden I. Computer Crimes and Digital Investigations / I. Walden. Oxford: Oxford University Press. 2016. 600 p

18 See, for example, Kirilenko, V. P., Alekseev, G. V. Political Technologies and International Conflict in the Information Space of the Baltic Region [Politicheskie tekhnologii i mezhdunarodnyi konflikt v informatsionnom prostranstve Baltiiskogo regiona] // Baltic Region [Baltiiskii region]. 2018. Vol. 10. No. 4. Pp. 20-38. DOI: 10.5922/2079-8555-2018-4-2. (in Russian) Kirilenko V.P., Shamakhov V.A., Alekseev G.V. Op. cit.

19 See, for example, Kirilenko, V. P., Alekseev, G. V. Actual Problems of Countering Extremist Crimes [Aktual'nye problemy protivodeistviya prestupleniyam ekstremistskoi napravlennosti] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. Vol. 12. No. 4. Pp. 561-571. DOI: 10.17150/2500-4255.2018.12 (4).561-571. (in Russian) P.8-18

20 Kirilenko, V. P., Alekseev, G. V. Extremists: Criminals and Victims of Radical Violence [Ekstremisty: prestupniki i zhertvy radikal'nogo nasiliya] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2019. Vol. 13. No. 4. Pp. 612-628. DOI: 10.17150/2500-4255.2019.13(4).612-628. (in Russian)

21 See: Nomokonov, V. A., Tropina, T. L. Cybercrime: Forecasts and Problems of Struggle [Kiberprestupnost': prognozy i problemy bor'by] // Criminalist Library [Biblioteka kriminalista]. 2013. № 5 (10). Pp. 148-160. (in Russian) Kirilenko V.P., Alekseev G.V. Op.cit. Supra note 8.

22 See: Reep-van den Bergh C. M. M., Junger M. Victims of Cybercrime in Europe: A Review of Victim Surveys // Crime Science. 2018. Vol. 7, art No. 5. DOI:10.1186/s40163-018-0079-3

23 Repetskaya, A. L. Current State, Structure and Trends of Russian Crime [Sovremennoe sostoyanie, struktura i tendentsii rossiiskoi prestupnosti] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo]. 2018. No. 1 (54). Pp. 151-156. DOI: 10.25513/1990-5173.2018.1.151-156. (in Russian)

24 Zhuravlenko, N. I., Shvedova, L. E. Problems of Combating Cybercrime and Promising Areas of International Cooperation in this Area [Problemy bor'by s kiberprestupnost'yu i perspektivnye napravleniya mezhdunarodnogo sotrudnichestva v etoi sfere] // Society and Law [Obshchestvo i pravo]. 2015. No. 3 (53). Pp. 66-70. (in Russian) P.69

25 Order of the President of the Russian Federation dated March 22, 2008 No. 144-rp [Online source]. URL: http://www.kremlin.ru/acts/bank/27059 (date of access: 22.02.2021).

entities»[26]. Private procedural issues often hinder the implementation of international agreements in the national legal system and, as follows from the political scandal over foreign interference in the US presidential election, cybersecurity issues can definitely affect the fundamentally important national interests of States[27]. Digital transformation undoubtedly requires the improvement of the institutions of international information law[28].

The controversial provisions of the Convention on Cybercrime allow states parties to «access, through a computer system in their territory, computer data stored in the territory of another Party, or to obtain it if that Party has the legal and voluntary consent of a person who has the legal authority to disclose this data to that Party through such a computer system» (art. 32), which in certain circumstances may be interpreted as a legal basis for interference in matters falling within the domestic jurisdiction of a State party to the agreement. However, non-adherence to the Budapest Convention leaves open the question of the compliance of the norms of the criminal legislation of the Russian Federation with international standards and the modernity of the provisions of Chapter 28 of the Criminal Code of the Russian Federation «Crimes in the field of computer information» (Article 272-274.1 of the Criminal Code of the Russian Federation). Criminalization of illegal influence on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation) does not fully reflect the substance of modern information technologies. The sovereignty of Russia in the information space is protected in accordance with the Federal Law of July 26, 2017. No. 187-FZ «On the security of the Critical Information Infrastructure of the Russian Federation», however, the criminal legislation does not define the concept of critical information infrastructure accurately enough, which creates legal uncertainty in the fight against cybercrime.

The classification of the material components of cybercrime does not cause fundamental differences in the documents of the Council of Europe, but it is an ambiguous problem in national criminal law. The 2001 Convention on Crimes in the Field of Computer Information identifies crimes against the confidentiality, integrity and availability of computer data and systems (Articles 2-6), offenses related to the use of computer tools (Articles 7-8), offenses related to the content of data (Article 9), offenses related to the violation of copyright and related rights (Article 10). Offences related to the manifestation of racism and xenophobia committed through computer systems obviously belong to the group of crimes related to the content of data. From the convention classification, it can be concluded that computer crimes can be committed both by subjects who use special knowledge in the field of computer programming technologies for criminal purposes, and by persons who use legal computer software to commit crimes. In particular, «the facts of the development of information technologies and computer networks by transnational terrorist and extremist organizations are increasingly noted, which led to the emergence of the most dangerous type of computer crime – cyberterrorism»[29], while it is obvious that cyberterrorism is associated not only with software modification, but also involves the recruitment of an audience of social networks and the promotion of extremism[30]. Computer fraud technologies are actively used to finance extremist activities and international terrorism.

In the Russian Federation, the qualification of theft under Article 159.6 of the Criminal Code of the Russian Federation «Fraud in the field of computer information» for a criminals who carried out illegal operations in a computer network (hacker) may entail the qualification of an act under the corresponding composition of Chapter 28 of the Criminal Code of the Russian Federation (an ideal set of crimes[31]), but this legal logic is not applied in practice[32]. Since hacker attacks can pursue not only economic, but also political motives[33], they are considered as a crime with a material composition and are qualified by their consequences.

Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 of November 30, 2017 «On judicial practice in cases of fraud, embezzlement and misuse» clarifies that «within the meaning of art. 159.6 of the Criminal Code of the Russian Federation interference in the functioning of means of storage, processing or transmission of computer information or information and telecommunications networks is recognized as the purposeful impact of software and (or) software and hardware on servers, computer equipment, including portable – laptops, tablet computers, smartphones equipped with appropriate software, or on information and telecommunications networks...» (paragraph 20). In fact, «if the theft of someone else's property ... is carried out by spreading deliberately false information in information and telecommunications networks,

---

[26] On signing the Convention on Cybercrime: Order of the President of the Russian Federation of November 15, 2005 No. 557-rp // Code of Law of the Russian Federation, 2005, No. 47, Article 4929

[27] See: Brenner S. W. Cyberthreats and the Decline of the Nation-State. London: Routledge. 2014. 182 p.; Justice J. W., Bricker B. J. Hacked: Defining the 2016 Presidential Election in the Liberal Media / J. W. Justice // Rhetoric and Public Affairs. 2019. Vol. 22, iss. 3. Pp. 389-420. DOI: 10.14321/rhetpublaffa.22.3.0389

[28] See: D'Aspremont J. Cyber Operations and International Law: An Interventionist Legal Thought // Journal of Conflict and Security Law. 2016. Vol. 21, iss. 3. Pp. 575-593. DOI: 10.1093/jcsl/krw022; Kettemann M. C. Ensuring Cybersecurity through International Law // Revista Espanola de Derecho Internacional. Vol. 69, iss. 2. Pp. 281-290

[29] Supra note 24. P. 67

[30] Supra note 11. P. 238

[31] Chernenko, T. G. The Qualification of the Aggregate of Crimes [Kvalifikatsiya sovokupnosti prestuplenii] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo.]. 2014. No. 1 (38). Pp. 148-162. (in Russian) P.151

[32] Engelhardt, A. A. On Understanding of Fraud in the Field of Computer Information // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2016. No. 8. Pp. 84-90. (in Russian) P.90

[33] See: Arnold N., Mahoney W., Derrick D., Ligon G. & Harms M. Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization // Journal of Information Warfare. 2015. Vol. 14, iss. 1. Pp. 84-100

including the Internet (for example, the creation of fake websites...), then such fraud should be qualified under Article 159, and not 159.6 of the Criminal Code of the Russian Federation» (paragraph 21).

The legal logic developed in the framework of the fight against economic cybercrimes has not found application in the practice of protecting other objects of criminal legal protection. In the Resolution of the Plenum of the Supreme Court of the Russian Federation of December 25, 2018 No. 46 «On certain issues of judicial practice in cases of crimes against the constitutional rights and freedoms of man and citizen...» it is noted that the dissemination of information about a person's private life consists in communicating (disclosing) it to one or more persons orally, in writing or in any other form and by any means (in particular, by transmitting materials or posting information using information and telecommunications networks, including the Internet) (paragraph 3), but the dissemination of information of limited access in a computer network does not constitute a special crime. Similar are the provisions of the Resolution of the Plenum of the Supreme Court of the Russian Federation No. 11 of June 28, 2011 «On judicial Practice in criminal cases of extremist crimes», which notes the possibility of bringing to criminal responsibility for public calls to carry out extremist activities on the Internet on the same legal grounds that were developed to bring to justice journalists who abuse freedom of speech (Part 2 of Article 280 of the Criminal Code of the Russian Federation). Provisions of the Federal Law of July 25, 2002 No. 114-FZ «On Countering extremist activities» is interpreted by the judicial authorities on the basis that the Internet, including websites, blogs and forums, is a private example of a public space.

The Resolution of the Plenum of the Supreme Court of the Russian Federation No. 16 of December 4, 2014 «On judicial practice in cases of crimes against sexual inviolability and sexual freedom of the individual» notes that «such actions may also be recognized as depraved, in which there was no direct physical contact with the body of the victim, including actions committed using the Internet or other information and telecommunications networks» (paragraph 17).

Resolution of the Plenum of the Supreme Court of the Russian Federation No. 14 of April 26, 2007 «On the practice of consideration by courts of criminal cases on Infringement of copyright, related, inventive and patent rights, as well as on the illegal use of a trademark» in the spirit of Article 10 of the Budapest Convention recognizes the possibility of committing crimes against intellectual property in computer networks (paragraph 4), but does not contain special rules and explanations for this type of cybercrimes.

The Resolution of the Plenum of the Supreme Court of the Russian Federation of June 15, 2006 No. 14 «On judicial practice in cases of crimes related to narcotic drugs, psychotropic, potent and toxic substances» (as amended on May 16, 2017) does not pay due attention to the threat of the distribution of narcotic drugs through computer communication networks and the promotion of the recreational use of psychoactive substances. There is every reason to believe that the threats posed by cybercrime are not fully assessed by law enforcement agencies, and this is happening not only in the Russian Federation, but also in other countries.

The experience of industrially developed countries demonstrates the technological dependence of all legislative initiatives in the online world[34]. Through legislative policies, countries such as Japan, South Korea, Australia, the Netherlands, and Germany are implementing harm reduction strategies (including from prohibitive measures) based on public-private partnerships to protect the «digital ecosystem»[35]. At the level of the European Union, national criminal legislation establishing responsibility for crimes in computer networks[36] is being harmonized, but «nonlegal factors such as national security, politics, the economy and public opinion encourage the spontaneous implementation of the European legal framework»[37]. The imperfection of European legislation is reflected in the high level of «shadow fraud», indicating that «the assessment of crime prevention based solely on police statistics may be inadequate».[38]

The Computer Misuse Act of 1990 is in force in the UK, which is aimed at combating cybercrime and is in many ways similar to Russian criminal law, but has certain specifics. On the one hand, the protection of computer systems and technologies from unauthorized access or modification always determines the object of encroachment of crimes that are associated with the use of computer technologies[39]. On the other hand, it is obvious that unlike Russian criminal law, which protects computer systems from harm, British statutes are initially more focused on protecting the rights of users of computer networks. The British lawmaker explains that the most common elements of cybercrimes involve unauthorized access to computer materials or unauthorized modification of computer programs and include: (1) hacking, including access to social network accounts and email passwords; (2) phishing – abuse of the trust of users in order to obtain passwords, security

34 See: Gercke M. Europe's Legal Approaches to Cybercrime // ERA Forum. 2009. Vol. 10. P. 409-420. DOI:10.1007/ S12027-009-0132-5

35 Dupont B. Bots, Cops, and Corporations: on the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime // Crime, Law and Social Change. 2017. Vol. 67, iss. 1. Pp. 97. DOI: 10.1007/s10611-016-9649-z

36 See: Buono L. Fighting Cybercrime between Legal Challenges and Practical Difficulties: EU and National Approaches // ERA Forum. 2016. Vol. 17. Pp. 343-353. DOI: 10.1007/s12027-016-0432-5

37 Calderoni F. The European Legal Framework on Cybercrime: Striving for an Effective Implementation // Crime, Law and Social Change. 2010. Vol. 54, iss. 5. P. 339. DOI: 10.1007/s10611-010-9261-6

38 Kemp S., Miro-Llinares F., Moneva A. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain// European Journal on Criminal Policy and Research. 2020. Vol. 26. DOI: 10.1007/s10610-020-09439-2

39 Karamnov, A. Yu., Dvoretsky, M. Yu. UK Legislation on Crimes in the Field of Computer Information [Zakonodatel'stvo Velikobritanii o prestupleniyakh v sfere komp'yuternoi informatsii] // Socio-Economic Phenomena and Processes [Sotsial'no-ekonomicheskie yavleniya i protsessy]. 2013. № 8 (54). Pp. 164-167. (in Russian)

information and personal data; (3) malware, including ransomware of various kinds[40], distributed denial of service attacks (DDOS) on websites, which are also accompanied by extortion[41].

In the United States of America, at the federal level, cybercrimes, in the sense of Russian criminal law, correspond most to the elements of crimes related to illegal access to communications and disruption of their normal operation (18 U.S.C. § 2701-2703), as well as the elements of causing damage to communication lines, stations or systems (18 U.S.C. § 1362). Special criminal protection of computer networks in the United States is carried out at the state level. Of particular importance for the international information space is the protective norm of art. 502 of the California Criminal Code[42], since the commercial Internet infrastructure is located in Silicon Valley under the jurisdiction of the state[43].

Federal law enforcement practice in the United States has long been based on the high public danger of cybercrime, but this initially concerned the protection of all technological systems of electrical communication (The Omnibus Crime Control and Safe Streets Act of 1968 [Wiretap Act] and Berger v. New York, 388 U.S. 41 (1967) Katz v. United States, 389 U.S. 347 (1967)). From United States v. Sutcliffe[44] explicitly follows the intention of the American judiciary to apply the logic of the analogy of the Retail Networks and Electrical Communications Act to the protection of information in computer networks, given that Congress has the necessary authority to regulate the Internet, as well as other tools and channels of interstate commerce (United States v. Hornaday, 392 F. 3d 1306, 1311).

Based on the logic of the economic nature of the Internet, in the United States, the most typical composition of cybercrimes is fraud associated with the dissemination of computer information of various kinds (18 U. S. C. § 1028, § 1028A, § 1029, § 1030, § 1037), special attention is paid to misleading domain names (18 U.S.C. § 2252B), as well as «words or digital images on the Internet» (18 U.S.C. § 2252C). The dissemination of prohibited information through computer networks in the United States is prosecuted on general grounds (18 U.S.C. 2252A), the same logic applies to criminal prosecution for copyright infringement in computer networks (17 U.S.C. § 506, 18 U.S.C. § 2319). The American legislator intentionally protects the physical communication infrastructure with the same legislative norms as the software, reasonably believing that the sanction (up to ten years in prison) is associated with an attempt to damage those computer systems at the national level that are particularly important for the state (in Russia, such systems are characterized as critical information infrastructure). Approaches to cybercrime in Russian and foreign criminal law largely coincide, but some fundamental issues are resolved taking into account the peculiarities of the sources of national law.

A discursive analysis of legislation and court decisions shows that in the context of digital transformation, it is necessary to protect a wide range of interests of high-tech corporations and their clients from criminal encroachments by criminal structures located within the state apparatus, the business community and public organizations. At the same time, American law enforcement practice demonstrates that the dissemination of information through computer communication networks, being a way of committing various crimes, is usually carried out by a subject who has access to official information, and should be qualified taking into account the motives of the criminal and the real consequences of the offense, without special attention to a specific method of obtaining access to classified information.

Well-known American lawyer Jeffrey L. Fisher, acting as a lawyer for Nathan Van Buren, a former police officer of the State of Georgia, who provided information from the police database to a friend for 6 thousand US dollars, rightly noted that the decision in the case of United States v. Van Buren[45] makes the violation of the usual restrictions on the processing of digital data a serious federal crime. The US Supreme Court, considering the question of whether real computer hacking is necessary for the prosecution of a computer crime, concluded that the actions constitute a crime if illegal access to computer information was obtained, the method of obtaining access is not essential for the qualification of the act. In turn, the case of Riley v. California[46] demonstrates the need to respect the interests of citizens in computer networks on the part of the state and especially protect the privacy of private life, given that everything «digital is different from the physical»[47]. US case law shows how «Supreme Court decisions have echoes far beyond the specific parties involved, even beyond the judicial system.»[48]

---

[40] Nasution M. D. T. P., Siahaan A. P. U., Rossanty Y., Aryza S. The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop // International Journal of Civil Engineering and Technology. 2018. Vol. 9, iss. 6. Pp. 1584-1585

[41] The Threat from Cyber Crime [Online source]. URL: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime (date of access: 22.02.2021)

[42] California Penal Code § 502. [Online source]. URL: http://leginfo.legislature.ca.gov/faces/codes_ displaySection.xhtml?lawCode=PEN&sectionNum=502 (date of access: 01.03.2021)

[43] Skinner C. P. Cybercrime in the Securities Market: Is U.C.C. Article 8 Prepared? // North Carolina Law Review Addendum. 2012. Vol. 90. Pp. 132-157. DOI: 10.2139/ssrn.1952955

[44] United States of America, Plaintiff-Appellee v. Steven William Sutcliffe, Defendant-Appellant, No. 04-50189, Decided: October 11, 2007 [Online source]. URL: https://caselaw.findlaw.com/us-9th-circuit/1166432.html (date of access: 01.03.2021)

[45] United States v. Van Buren. No. 18-12024 (11th Cir. 2019) [Online source]. URL: https://law.justia. com/cases/federal/appellate-courts/ca11/18-12024/18-12024-2019-10-10.html (date of access: 01.03.2021)

[46] Supreme Court of the United States Syllabus. Riley v. California [Online source]. URL: https://www. supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf (date of access: 01.03.2021)

[47] Faculty on Point: Prof. Jeffrey Fisher on Digital Privacy and the Riley Decision [Online source]. URL: https://law.stanford.edu/directory/jeffrey-l-fisher/ffslsnav-featured-video (date of access: 01.03.2021)

[48] Fisher J. L. A Clinic's Place in the Supreme Court Bar // Stanford Law Review. 2013 (2011). Vol. 65, iss. 1. P. 137. DOI: 10.2139/ssrn.1921430

After the idea of expanding the ability of US law enforcement agencies to combat foreign-registered websites, online copyright infringement, and illegal trafficking of counterfeit goods on the Internet came to a standstill in 2012, and the SOPA (Stop Online Piracy Act – the Anti-Piracy Law) and the PIPA (Protect IP Act) were rejected, and it became clear that the economic interests of corporations are subordinated to the system-forming principles of a virtual environment where freedom of speech and innovation dominate, and any Internet censorship will be met with a strong protest from the online community[49].

Progressive Russian studies confirm that «the state is obliged not to ignore the «online problems», but to deal with them closely, otherwise private companies – manufacturers of online worlds will begin to set the «rules of the game».»[50] In the online space, deception does not become the norm, but the ways of disguising fraud technologies as creative solutions, as well as information warfare, acquire the character of a socio-political international technology[51]. On the one hand, the technical understanding of the fundamental differences between the actions of creative digitalization guerrillas and classic crimes of an extremist nature reflects the need to develop special norms to ensure the rule of law in the global information space[52]. On the other hand, the danger of creative projects is only indirectly related to their technical implementation, since online reality can carry unpredictable socio-psychological and economic threats[53].

Cybercrime, based on the technological features of the implementation of the criminal plan, can cover an indefinite range of persons – recipients of potentially dangerous messages[54]. For high-tech industries, the general rules of criminal law are not always acceptable. In Russian legal science, there is also an understanding that «the existing legal mechanisms are not always feasible for Internet relations»[55] and, in particular, the legislation does not effectively protect the rights of consumers of computer software[56]. It is obvious that cybercrime is embedded in a variety of organizational structures and is focused on making a profit by violating the rights of the general population[57]. Providing access to potential victims of crime is often carried out by creating various social and technological networks on the Internet[58], empirical data within which is quite difficult to collect, and the unknown, indeed, can generate panic around an unprotected Internet audience[59].

Some high-profile cybercrimes did not harm the critical information infrastructure, and some serious serious crimes were not solved, for example, the creators of the WannaCry virus were never exposed and brought to justice, which means that their economic or political motives were not established. The reasonable qualification of cybercrimes largely depends on the objective side of their composition. Two cybercrimes similar to the object of encroachment can be distinguished by a fundamentally different public danger. For example, an American student, Varun H. Sarja, hacked into several computers at an educational institution, changed his grades and was sentenced to one and a half years of probation[60]. At the same time, the British hacker Alex Bessell was sentenced to two years in prison for a formally similar crime – systematic cyber attacks, carrying out which he earned more than 50 thousand pounds[61]. Both cases demonstrate the existence of significant

---

49 See: Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / D. Moon, P. Ruffini, D. Segal (eds). OR Books. 2013. 316 p.; Kapczynski A. Intellectual Property's Leviathan // Law and Contemporary Problems. 2015. Vol. 77, iss. 4. Pp. 131-145

50 Baturin, Yu. M., Polubinskaya, S. V. What Makes Virtual Crimes Real [Chto delaet virtual'nye prestupleniya real'nymi] // Proceedings of the Institute of State and Law of the Russian Academy of Sciences [Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk]. 2018. V. 13. No. 2. Pp. 9-35. (in Russian) P.30

51 Kirilenko V.P., Alekseev G.V. Po. cit. Supra note 8, 18

52 See: Taylor R. W., Fritsch E. J., Liederbach J. Digital Crime and Digital Terrorism. New York: Prentice Hall Press, 2014. 416 p

53 Baturin Yu.M., Polubinskaya S.V. Op.cit. Supra note 50

54 See: Cooper M. How Cyber Crime Damages Lives // ITNOW. 2020. Vol. 62, iss. 1. Pp. 36-37. DOI: 10.1093/ itnow/bwaa016; De Silva S. Cyber Crime and the Law // ITNOW. 2016. Vol. 58, iss. 4. Pp. 28-29. DOI: 10.1093/ itnow/bww101; Dalgaard-Nielsen A. Supra note 17; Walden I. Supra note 17

55 Zharova, A. K. Routing and IP to Ensure the Legal Regulation of Internet Relations [Marshrutizatsiya i IP dlya obespecheniya pravovogo regulirovaniya internet-otnoshenii] // Bulletin of the Russian State Humanitarian University. Series «Informatics. Information Security. Mathematics» [Vestnik RGGU. Seriya «Informatika. Informatsionnaya bezopasnost'. Matematika»]. 2019. No. 2. Pp. 32-42. DOI: 10.28995/2686-679X-2019-2-32-42. (in Russian) P.40

56 See: Zharova A. Ensuring the Information Security of Information Communication Technology Users in Russia // International Journal of Cyber Criminology. 2019. Vol. 13, iss. 2. Pp. 255-269

57 See: Leukfeldt E. R., A. Lavorgna, E.R. Kleemans. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime // European Journal on Criminal Policy and Research. 2017. Vol. 23, iss. 3. P. 287-300. DOI:10.1007/s10610-016-9332-z; Broadhurst R. G., P. Grabosky, M. Alazab. Supra note 5

58 Ivantsov, S. V., Borisov, S. V., Uzembaeva, G. I., Muzychuk, T. L., Tishchenko, Yu. Yu. Actual Problems of Improving the System of Measures for Criminological Prevention of Extremist Crimes Committed Using Information and Telecommunication Networks [Aktual'nye problemy sovershenstvovaniya sistemy mer kriminologicheskogo preduprezhdeniya prestuplenii ekstremistskoi napravlennosti, sovershaemykh s ispol'zovaniem informatsionno- telekommunikatsionnykh setei] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 776-784. DOI: 10.17150/2500-4255.2018.12(6).776-784 (in Russian)

59 See: Lavorgna A. Cyber-Organised Crime. A Case of Moral Panic? // Trends in Organized Crime. 2019. Vol. 22, iss. 4. Pp. 357-374. DOI: 10.1007/s12117-018-9342-y.

60 Former University of Kansas Student Gets Probation for Changing Failing Grades to 'A' Via Hacking [Online source]. URL: https://www.indiawest.com/news/global_indian/former-university-of-kansas-student-gets-probation-for-changing-failing/article_07766628-7f0d-11e8-8d2a-3bf0c388ace0.html (date of access: 20.02.2021)

61 Hacker Alex Bessell Jailed for Cyber Crime Offences [Online source]. URL: https://www.bbc.com/news/ uk-england-42733638 (date of access: 20.02.2021)

problems in the court's assessment of the real damage caused by illegal actions in computer networks. The criminal prosecution of US Senator Anthony D. Weiner for indecent acts in social networks in relation to a minor victim demonstrated that health problems, assistance to the investigation and good behavior can lead to an actual sentence of one and a half years of compulsory treatment with subsequent measures of additional punishment[62].

The practice of law enforcement confirms that when qualifying cybercrimes and assigning penalties for their commission, a legal assessment of the consequences of the offense is carried out, that is, online crimes are considered by the court as crimes with material composition, while the degree of guilt of the online delinquent may be characterized by indirect intent, and the methods of committing crimes will be increasingly influenced by artificial intelligence[63]. The motives for the destruction of virtual infrastructure can be dictated by the logic inherent in international crimes against cultural heritage, and cover both the Herostratus complex and extremist beliefs that lead to discrimination[64].

The presumption of innocence of all participants in online communication is of great importance in the system of assessing the public danger of cybercrime, but it is common for subjects who commit serious crimes in the online world to disguise their actions as the sale of goods, services and intellectual rights, as well as under voluntary donations from citizens for the development of their projects. When identifying cyberdelicts, the grounds for doubts about the legality of the functioning of Internet sites can serve as clear signs of the presence of the right of violation, as well as complaints from users of a network resource about the violation of their subjective rights. Obviously, it is the victims complaints that can reveal fraud, propaganda of extremism and other cybercrimes, while revealing the modus operandi of the virtual delinquent. Fraudulent websites, online casinos, and death groups on social networks often use identical techniques to phish personal data and gain control over the actions of the victim of the crime. There is every reason to believe that the organized criminal communities that exist in the virtual space, acting out of selfish and extremist motives, sooner or later become involved in the struggle for power and political influence, abusing the trust of Internet users.

Conclusion. Digital transformation expands the possibilities of active subjects of legal relations in all spheres of modern society, but the introduction of information technologies in the national economy in practice often causes serious social problems. On the one hand, in the process of digitalization, there are many new opportunities for creativity, organizing communication, modeling virtual reality and implementing ambitious technical projects. On the other hand, as a result of digital transformation, new aspects in the activities of criminal communities are also emerging. First, criminal communities use information networks to recruit new members to their ranks and motivate individual members of society to take actions that contribute to the achievement of criminal goals. Secondly, a significant part of the proceeds from fraud in the field of computer information for various reasons of a purely criminal nature can be directed to the financing of extremist activities. Thirdly, there is a threat of criminalization of cyberspace, where organized crime is developing, criminal network resources are flourishing, such as: information systems for finding performers of criminal services and paying for them, resources for providing access to classified and counterfeit information, sites for selling fake and low-quality goods, online casinos and various fraudulent political projects that abuse the trust of citizens.

Substantive criminal law is significantly lagging behind in its development from those criminal schemes that are actively developed and implemented in the life of the network community. It is necessary to introduce new types of additional criminal penalties that can restrict the rights of citizens to participate in online communication, including bans: on the use of social networks, on the creation of network sites, on the use of numbering resources of the global network. In cases where criminal activity in the information space is of a cross-border nature, the harmonization of criminal legislation and international police cooperation become critical elements of information security.

The system for assessing the public danger of cybercrime should be based on taking into account the harm caused to the legally protected interests of all users of network resources, as well as on the timeliness of unmasking the criminal intent by law enforcement agencies. The central element of the critical information infrastructure of each state remains the user of computer systems, and it is the user who is least protected by criminal law in the process of digital transformation of all spheres of society.

Given the fact that «there is a lot of theoretical reasoning about the fear of sanctions that motivates people not to violate legal obligations,»[65] it is obvious that the digital transformation is changing the perception of the threat of punishment by most users of computer networks. The energy of virtual things (the Internet of things)[66] and the commodification of computer communication have a significant impact on the activity of criminal structures, which in the new conditions seek to solve their own criminal and political problems with the help of digital technologies in the virtual space of computer networks. The

---

62 Anthony Weiner Released from Prison After Serving 18 months for Sexting Teenager [Online source]. URL: https://www.nytimes.com/2019/05/14/nyregion/anthony-weiner-prison-release.html (date of access: 20.02.2021)

63 See: Begishev I.R., Khisamova Z.I. Op.cit. Supra note 4; Van der Wagen W. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks // British Journal of Criminology. 2015. Vol. 55, iss. 3. Pp. 578-595. DOI: 10.1093/bjc/azv009

64 See: Brosche J., Legner M., Kreutz J., Ijla A. Heritage under Attack: Motives for Targeting Cultural Property During Armed Conflict // International Journal of Heritage Studies 2017. Vol. 23, iss. 3. Pp. 248-260. DOI: 10.1080/13527258.2016.1261918

65 See: Nuotio K. A Legitimacy-Based Approach to EU Criminal Law: Maybe We Are Getting There, After All // New Journal of European Criminal Law. 2020. Vol. 11, iss. 1. P. 24. DOI: 10.1177/2032284420903386

66 See: Mylrea M. Smart Energy-Internet-of-Things Opportunities Require Smart Treatment of Legal, Privacy and Cybersecurity Challenges // The Journal of World Energy Law & Business. 2017. Vol. 10, iss. 2. Pp. 147-158. DOI: 10.1093/jwelb/jwx001

growing opportunities for the use of artificial intelligence in the interests of criminal communities emphasize the importance of adjusting the criminal policy of developed countries in the direction of protecting the ideals of humanism and protecting the status of the individual, who is increasingly vulnerable in the competition between human and machine intelligence. There is no doubt that criminal law mechanisms are necessary to prevent digital slavery and the devaluation of human labour.

References

1. Ammar, J. Cyber Gremlin: Social Networking, Machine Learning and the Global War on Al-Qaida and IS-Inspired Terrorism // International Journal of Law and Information Technology. 2019. Vol. 27, iss. 3. Pp. 238-265. DOI: 10.1093/ijlit/eaz006.
2. Arnold, N., Mahoney, W., Derrick, D., Ligon, G. & Harms, M. Feasibility of a Cyber Attack on National Critical Infrastructure by a Non-State Violent Extremist Organization // Journal of Information Warfare. 2015. Vol. 14, iss. 1. Pp. 84-100.
3. Awan, I. Cyber-Extremism: Isis and the Power of Social Media // Social Science and Public Policy 2017. Vol. 54. Pp. 138-149. DOI: 10.1007/s12115-017-0114-0.
4. Bastrykin, A. I. Crimes Against Minors in the Internet Space: On the Issue of Victimological Prevention and Criminal-Legal Assessment [Prestupleniya protiv nesovershennoletnikh v internet-prostranstve: k voprosu o viktimologicheskoi profilaktike i ugolovno-pravovoi otsenke] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2017. Vol. 11. No. 1. Pp. 5-12. DOI: 10.17150/2500-4255.2017.11 (1).5-12. (in Russian)
5. Baturin, Yu. M., Polubinskaya, S. V. What Makes Virtual Crimes Real [Chto delaet virtual'nye prestupleniya real'nymi] // Proceedings of the Institute of State and Law of the Russian Academy of Sciences [Trudy Instituta gosudarstva i prava Rossiiskoi akademii nauk]. 2018. V. 13. No. 2. Pp. 9-35. (in Russian)
6. Begishev, I. R. Khisamova, Z. I. Criminological Risks of Using Artificial Intelligence [Kriminologicheskie riski primeneniya iskusstvennogo intellekta] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 767-775. DOI: 10.17150 / 2500-4255.2018.12 (6). 767-775. (in Russian)
7. Brenner, S. W. Cyberthreats and the Decline of the Nation-State. London: Routledge. 2014. 182 p.
8. Broadhurst, R. G., P. Grabosky, M. Alazab, S. Chon. Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime // International Journal of Cyber Criminology. 2014. Vol. 8, iss. 1. Pp. 1-20. DOI: 10.2139/ssrn.2345525.
9. Brosche, J., Legner, M., Kreutz, J., Ijla, A. Heritage under Attack: Motives for Targeting Cultural Property During Armed Conflict// International Journal of Heritage Studies 2017. Vol. 23, iss. 3. Pp. 248-260. DOI: 10.1080/13527258.2016.1261918.
10. Buono, L. Fighting Cybercrime Between Legal Challenges and Practical Difficulties: EU and National Approaches // ERA Forum. 2016. Vol. 17. Pp. 343-353. DOI: 10.1007/s12027-016-0432-5.
11. Calderoni, F. The European Legal Framework on Cybercrime: Striving for an Effective Implementation // Crime, Law and Social Change. 2010. Vol. 54, iss. 5. Pp. 339-357. DOI: 10.1007/s10611-010-9261-6.
12. Chernenko, T. G. The Qualification of the Aggregate of Crimes [Kvalifikatsiya sovokupnosti prestuplenii] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo.]. 2014. No. 1 (38). Pp. 148-162. (in Russian)
13. Cooper, M. How Cyber Crime Damages Lives // ITNOW. 2020. Vol. 62, iss. 1. Pp. 36-37. DOI: 10.1093/itnow/ bwaa016.
14. D'Aspremont, J. Cyber Operations and International Law: An Interventionist Legal Thought // Journal of Conflict and Security Law. 2016. Vol. 21, iss. 3. Pp. 575-593. DOI: 10.1093/jcsl/krw022.
15. Dalgaard-Nielsen, A. Violent Radicalization in Europe: What We Know and What We Do Not Know // Stud Conflict Terrorism 2010. Vol. 33, iss. 9. Pp. 797-814. DOI: 10.1080/1057610X.2010.501423.
16. De Silva, S. Cyber Crime and the Law // ITNOW 2016. Vol. 58, iss. 4. Pp. 28-29. DOI: 10.1093/itnow/bww101.
17. Dupont, B. Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation As a Way to Control Large-Scale Cybercrime // Crime, Law and Social Change. 2017. Vol. 67, iss. 1. Pp. 97-116. DOI: 10.1007/s10611-016-9649-z.
18. Earl, J. Protest Online: Theorizing the Consequences of Online Engagement. In L. Bosi, M.Giugni & K. Uba (eds.). The Consequences of Social Movements. Cambridge: Cambridge University Press. 2016. Pp. 363-400. DOI: 10.1017/CBO9781316337790.015.
19. Engelhardt, A. A. On Understanding of Fraud in the Field of Computer Information // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2016. No. 8. Pp. 84-90. (in Russian)
20. Fisher, J. L. A Clinic's Place in the Supreme Court Bar // Stanford Law Review. 2013 (2011). Vol. 65, iss. 1. Pp. 137-201. DOI: 10.2139/ssrn.1921430.
21. Gercke, M. Europe's Legal Approaches to Cybercrime // ERA Forum. 2009. Vol. 10. Pp. 409-420. DOI: 10.1007/s12027-009-0132-5.
22. Hacking Politics: How Geeks, Progressives, the Tea Party, Gamers, Anarchists and Suits Teamed up to Defeat SOPA and Save the Internet / D. Moon, P. Ruffini, D. Segal (eds). OR Books. 2013. 316 p.

23. Ivantsov, S. V., Borisov, S. V., Uzembaeva, G. I., Muzychuk, T. L., Tishchenko, Yu. Yu. Actual Problems of Improving the System of Measures for Criminological Prevention of Extremist Crimes Committed Using Information and Telecommunication Networks [Aktual'nye problemy sovershenstvovaniya sistemy mer kriminologicheskogo preduprezhdeniya prestuplenii ekstremistskoi napravlennosti, sovershaemykh s ispol'zovaniem informatsionno-telekommunikatsionnykh setei] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. T. 12, No. 6. Pp. 776-784. DOI: 10.17150/2500-4255.2018.12(6).776-784 (in Russian)
24. Justice, J. W., Bricker, B. J. Hacked: Defining the 2016 Presidential Election in the Liberal Media / J. W. Justice // Rhetoric and Public Affairs 2019. Vol. 22, iss. 3. Pp. 389-420. DOI: 10.14321/rhetpublaffa.22.3.0389.
25. Kapczynski, A. Intellectual Property's Leviathan // Law and Contemporary Problems. 2015. Vol.77, iss. 4. Pp. 131-145.
26. Karamnov, A. Yu., Dvoretsky, M. Yu. UK Legislation on Crimes in the Field of Computer Information [Zakonodatel'stvo Velikobritanii o prestupleniyakh v sfere komp'yuternoi informatsii] // Socio-Economic Phenomena and Processes [Sotsial'no-ekonomicheskie yavleniya i protsessy]. 2013. № 8 (54). Pp. 164-167. (in Russian)
27. Kemp, S., Miro-Llinares, F., Moneva, A. The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain // European Journal on Criminal Policy and Research. 2020. Vol. 26. DOI: 10.1007/s10610-020-09439-2.
28. Kettemann, M. C. Ensuring Cybersecurity through International Law // Revista Espanola de Derecho Internacional. Vol. 69, iss. 2. Pp. 281-290.
29. Kirilenko, V. P., Alekseev, G. V. Actual Problems of Countering Extremist Crimes [Aktual'nye problemy protivodeistviya prestupleniyam ekstremistskoi napravlennosti] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2018. Vol. 12. No. 4. Pp. 561-571. DOI: 10.17150/2500-4255.2018.12 (4).561-571. (in Russian)
30. Kirilenko, V. P., Alekseev, G. V. Harmonization of Russian Criminal Legislation on Combating Cybercrime with the Legal Standards of the Council of Europe [Garmonizatsiya rossiiskogo ugolovnogo zakonodatel'stva o protivodeistvii kiberprestupnosti s pravovymi standartami Soveta Evropy] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2020. Vol. 14. No. 6. Pp. 898-913. DOI: 10.17150/2500-4255.2020.14(6).898-913. (in Russian)
31. Kirilenko, V. P., Alekseev, G. V. The Legitimacy of Democracy in the Works of Max Weber and Karl Schmitt [Legitimnost' demokratii v rabotakh Maksa Vebera i Karla Shmitta] // Jurisprudence [Pravovedenie]. 2018. Vol. 62. No. 3. Pp. 501-517. DOI: 10.21638/11701/spbu25.2018.305. (in Russian)
32. Kirilenko, V. P., Alekseev, G. V. Political Technologies and International Conflict in the Information Space of the Baltic Region [Politicheskie tekhnologii i mezhdunarodnyi konflikt v informatsionnom prostranstve Baltiiskogo regiona] // Baltic Region [Baltiiskii region]. 2018. Vol. 10. No. 4. Pp. 20-38. DOI: 10.5922/2079-8555-2018-4-2. (in Russian)
33. Kirilenko, V. P., Alekseev, G. V. Counteracting the Ideology of Modern Terrorism [Protivodeistvie ideologii sovremennogo terrorizma] // Administrative Consulting [Upravlencheskoe konsul'tirovanie]. 2018. No. 5 (113). Pp. 8-18. DOI: 10.22394/1726-1139-2018-5-8-18. (in Russian)
34. Kirilenko, V. P., Alekseev, G. V. Extremists: Criminals and Victims of Radical Violence [Ekstremisty: prestupniki i zhertvy radikal'nogo nasiliya] // Russian Journal of Criminology [Vserossiiskii kriminologicheskii zhurnal]. 2019. Vol. 13. No. 4. Pp. 612-628. DOI: 10.17150/2500-4255.2019.13(4).612-628. (in Russian)
35. Kirilenko, V. P., Shamakhov, V. A., Alekseev G. V. Freedom of Speech and Media Safety [Svoboda slova i mediabezopasnost']. SZIU RANEPA. St. Petersburg. 2019. 440 p. (in Russian)
36. Lavorgna, A. Cyber-Organised Crime. A Case of Moral Panic? // Trends in Organized Crime. 2019. Vol.22, iss. 4. Pp. 357-374. DOI: 10.1007/s12117-018-9342-y.
37. Leukfeldt, E. R., A. Lavorgna, E. R. Kleemans. Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime // European Journal on Criminal Policy and Research. 2017. Vol. 23, iss. 3. Pp. 287-300. DOI: 10.1007/s10610-016-9332-z.
38. Martin, J., Munksgaard, R., Coomber R. & oths. Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards // British Journal of Criminology. 2020. Vol. 60, iss. 3. Pp. 559-578. DOI: 10.1093/bjc/azz075.
39. Mylrea, M. Smart Energy-Internet-of-Things Opportunities Require Smart Treatment of Legal, Privacy and Cybersecurity Challenges // The Journal of World Energy Law & Business. 2017. Vol. 10, iss. 2. Pp. 147-158. DOI: 10.1093/jwelb/jwx001.
40. Nasution, M. D. T. P., Siahaan, A. P. U., Rossanty, Y., Aryza, S. The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop // International Journal of Civil Engineering and Technology. 2018. Vol. 9, iss. 6. Pp. 1583-1592.
41. Nomokonov, V. A., Tropina, T. L. Cybercrime: Forecasts and Problems of Struggle [Kiberprestupnost': prognozy i problemy bor'by] // Criminalist Library [Biblioteka kriminalista]. 2013. № 5 (10). Pp. 148-160. (in Russian)
42. Nuotio, K. A Legitimacy-Based Approach to EU Criminal Law: Maybe We Are Getting There, After All // New Journal of European Criminal Law. 2020. Vol. 11, iss. 1. Pp. 20-39. DOI: 10.1177/2032284420903386.
43. Odintsova, N. E., Repetskaya, A. L. Problematic Aspects of Domestic and Foreign Legislation in Countering the Propaganda of Pedophilia [Problemnye aspekty otechestvennogo i zarubezhnogo zakonodatel'stva v protivodeistvii propagande pedofilii] // International Journal of Humanities and Natural Sciences [Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk]. 2019. No. 11-3 (38). Pp. 84-89. DOI: 10.24411/2500-1000-2019-11821. (in Russian)

44. Reep-van den Bergh, C. M. M., Junger M. Victims of Cybercrime in Europe: A Review of Victim Surveys // Crime Science. 2018. Vol. 7, art No. 5. DOI: 10.1186/s40163-018-0079-3.
45. Repetskaya, A. L. Current State, Structure and Trends of Russian Crime [Sovremennoe sostoyanie, struktura i tendentsii rossiiskoi prestupnosti] // Bulletin of Omsk University. Series: Law [Vestnik Omskogo universiteta. Seriya: Pravo]. 2018. No. 1 (54). Pp. 151-156. DOI: 10.25513/1990-5173.2018.1.151-156. (in Russian)
46. Rucht, D. Movement Allies, Adversaries, and Third Parties. 2007. DOI: 10.1002/9780470999103.ch9.
47. Schmitt, Carl. Theorie des Partisanen. Zwischenbemerkung zum Begriff des Politischen. Duncker & Humblot. 1963.
48. Skinner, C. P. Cybercrime in the Securities Market: Is U.C.C. Article 8 Prepared? // North Carolina Law Review Addendum. 2012. Vol. 90. Pp. 132-157. DOI: 10.2139/ssrn.1952955.
49. Tarrow, S. Power in Movement: Social Movements, Collective Action and Politics. New York: Cambridge University Press. 1994. 251 p.
50. Taylor, R. W., Fritsch, E. J., Liederbach, J. Digital Crime and Digital Terrorism. New York: Prentice Hall Press, 2014. 416 p.
51. Tomasevic, V., Ilic-Kosanovic, T., Ilic, D. (2020) Skills Engineering in Sustainable Counter Defense Against Cyber Extremism. In: Al-Masri A., Al-Assaf Y. (eds.) Sustainable Development and Social Responsibility. Vol. 2. Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development). Springer, Cham. DOI: 10.1007/978-3-030-32902-0_25.
52. Van der Wagen, W. From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks // British Journal of Criminology. 2015. Vol. 55, iss. 3. Pp. 578-595. DOI: 10.1093/bjc/azv009.
53. Walden, I. Computer Crimes and Digital Investigations / I. Walden. Oxford: Oxford University Press. 2016. 600 p.
54. Zharova, A. Ensuring the Information Security of Information Communication Technology Users in Russia // International Journal of Cyber Criminology. 2019. Vol. 13, iss. 2. Pp. 255-269.
55. Zharova, A. K. Routing and IP to Ensure the Legal Regulation of Internet Relations [Marshrutizatsiya i IP dlya obespecheniya pravovogo regulirovaniya internet-otnoshenii] // Bulletin of the Russian State Humanitarian University. Series «Informatics. Information Security. Mathematics» [Vestnik RGGU. Seriya «Informatika. Informatsionnaya bezopasnost'. Matematika»]. 2019. No. 2. Pp. 32-42. DOI: 10.28995/2686-679X-2019-2-32-42. (in Russian)
56. Zhuravlenko, N. I., Shvedova, L. E. Problems of Combating Cybercrime and Promising Areas of International Cooperation in this Area [Problemy bor'by s kiberprestupnost'yu i perspektivnye napravleniya mezhdunarodnogo sotrudnichestva v etoi sfere] // Society and Law [Obshchestvo i pravo]. 2015. No. 3 (53). Pp. 66-70. (in Russian)