Research article
DOI: https://doi.org/10.21202/jdtl.2023.28

Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security

Evgeniy A. Russkevich

Kutafin Moscow State Law University
Moscow, Russian Federation

Keywords

Communication network,
communication operator,
criminal liability,
cyber resilience,
cybercrime,
digital technologies,
information security,
Internet,
law,
legislation

Abstract

Objective: to acquire new knowledge about the liability for violating the rules of managing technical means of counteracting the threats to information security; to elaborate theoretical recommendations and proposals for improving legislation and law enforcement.

Methods: the methodological basis of the research is a set of scientific cognition methods, including abstract-logic, dogmatic, comparison, etc.

Results: based on studying documents and publications, the following conclusions were made: 1) the measures taken at the national level for regulating the relations associated with introduction of technical means of counteracting the threats generally comply with the provisions of the Doctrine on information security of the Russian Federation; 2) one of the main directions of development of the foreign legislation on telecommunications is building a system of public-private interaction, in which communication operators would perceive the information security problem not as their internal task but as an element of the overall security of the state. In this regard, one may clearly trace the statement of the need to efficiently control the activities of communication operators, first of all, in the sphere of the newly introduced standards providing cyber resilience; 3) regulation of relations in the sphere of managing the technical means of counteracting threats in Russia is characterized by their multiplicity, multi-leveledness,

hence, rather predictable complexity; 4) the model of communication operators' liability for violations in the field of exploitation of technical means of counteracting threats, implemented in Article 274.2 Of the Russian Criminal Code, is not optimal. Rather disputable is the approach to describing the administratively prejudicial elements of crime. Despite the significance of the relations, the possibility of a criminal-legal reaction to a particular incident appears not in connection with the occurrence of certain publicly dangerous consequences and not even with the traditional recurrence, but only with the third documented violation. We consider more preferable the model of criminalization of violating the management of technical means of counteracting threats depending on infliction of substantial harm to the rights and legal interests of citizens or organizations, or the legally protected interests of the society or the state.

Scientific novelty: the novelty of the research is mainly due to the actual underdevelopment of the issues related to the legal definition and implementation of criminal liability for violating the rules of centralized management of technical means of counteracting the threats to sustainability, security and integrity of functioning of the telecommunication network Internet and the general purpose communication network in the territory of the Russian Federation.

Practical significance: the main provisions and conclusions of the research can be used for improving the mechanism of criminal-legal protection of information security, further development of the Russian doctrine of criminal law on liability for crimes in the sphere of computer information.

For citation

Russkevich, E. A. (2023). Violating the Rules of Centralized Management of Technical Means of Counteracting the Threats to Information Security. *Journal of Digital Technologies and Law, 1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

Contents

Introduction

Digital world is both the present and future of the humanity. Our everyday activity inevitably implies interacting with devices and technologies which rapidly change the idea of the reality. Through accounts, the digital alter egos, a person communicates, performs labor activity, receives services, and purchases goods. As a result, a modern person finds themselves in a position of a parallel being – physical and virtual. One can distance oneself from it, slow down digitalization in a certain sense, but the inevitability and irreversibility of the process makes us put a question: why do it? Answering this question, some researchers point out the negative consequences of introducing telecommunication technologies from the viewpoint of the state and dynamics of crime and its changed characteristics. As a rule, they demonstrate virtualization of the mechanisms of criminal turnover of illegal items, which significantly complicates the activity of law enforcement bodies. Also, they rather thoroughly explain that the development of some research directions (for example, in the sphere of artificial intelligence and robotics) bears a definite threat to humanity as a whole.

The above said is rather true in a certain sense. However, it is also true that this discourse in general does not go beyond confusion, traditional for the humanity, in front of something new, unexplored, the nature and probable impact of which are not completely clear. Any technology can be used for criminal purposes. This, however, cannot cancel progress as such, i. e. the human striving to arrange life in the most reasonable way. For this reason, one should speak not of protection humans against technologies but of building a model of technologies protection or, to be more precise, the model of legal provision of information-telecommunication development, which would allow preventing and adequately reacting to particular criminal infringements. In this sense, it is rather logical to focus on the issues of qualitative provision of sustainability of digital networks in relation to negative impacts, or their cyber resilience.

By Federal Law of July 14, 2022, No. 260-FZ "On making amendments in the Criminal Code of the Russian Federation and Criminal-Procedural Code of the Russian Federation", Chapter 28 of the Criminal Code of the Russian Federation[1] (further – CC RF) was complemented with a new norm, stipulating liability for violation of special rules of managing technical means providing normal functioning of the Internet and communication networks of general use in the territory of the state (Article 274.2 CC RF). The draft law passport does not allow acquainting with the justification of the implemented legislative initiative, as in the original edition Article 274.2 CC RF was not included. The respective amendments

[1] Criminal Code of the Russian Federation of June 13, 1996, No. 63-FZ. (1996, June 17). *Collection of legislation of the Russian Federation*, *25*, Article 2954.

appeared only by the second reading of the draft law[2]. Meanwhile, it is very important not only to comprehend the reasons for criminalizing certain violations associated with managing technical means of counteracting threats (further – TMCT) but also to analyze the legal-technical features of Article 274.2 CC RF, identify its advantages and possible drawbacks.

1. Methods of researching violations of the rules of centralized management of technical means of counteracting the threats to information security

The methodological tools of the research represent a complex combination of philosophical, general scientific and specific scientific means of cognition. The general scientific methods of cognition used in the work include analysis, synthesis, deduction, induction, classification, structural-functional method, etc. Special attention was paid to systemic method, which served as a starting prerequisite for solving the set tasks.

Empirical methods (analysis of documents, printed and electronic publications) were used for accumulating and studying the research materials. In the process of the article preparation, a letter to the federal unitary enterprise "General radio frequency centre"[3] (further – GRFC) was sent in order to obtain clarification about TMCT (an official response was received on December 25, 2022).

As for the specific scientific methods of cognition, they included comparative-legal, formal-legal (dogmatic), etc. The formal-legal method was used when studying normative-legal acts of the Russian Federation in the sphere of regulation and protection of information relations, Russian and foreign criminal legislation. The dogmatic method allowed solving a number of research tasks, for example, revealing the legal-technical definition of the elements according to Article 274.2 CC RF.

2. Information security and technical means of counteracting the threats

To comprehend the processes resulting in the Russian criminal legislation receiving a special norm of liability for violation of the centralized management of TMCT (Article 274.2 CC RF), one should, first of all, turn to the category of information security and strategic planning documents in this sphere.

---

2 Draft law No. 130406-8 "On making amendments in the Criminal Code of the Russian Federation and Criminal-Procedural Code of the Russian Federation" (with a view of improving criminal-legal protection of the national interests of the Russian Federation, rights and freedoms of citizens against new forms of criminal activity and threats to public security). https://sozd.duma.gov.ru/bill/130406-8

3 GRFC is a departmental expert center providing execution of the tasks and functions imposed on the radio frequency service, as well as support of control-surveillance and regulatory functions of Roskomnadzor by the main directions of its activity in the sphere of communication, mass media and mass communications. https://grfc.ru

In the Russian scientific literature, the notion of information security is rather well elaborated[4]. M. A. Efremova justly emphasizes that information security is a dynamic system of public relations. The openness of this system is due to the fact that information security cannot be of a constant, unchangeable character (Efremova, 2018).

The category of information security (in a narrower sense – cyber resilience) is also well studied in foreign literature (Colding et al., 2020; Espinoza-Zelaya & Moon, 2022; Hausken, 2020; Li et al., 2020; Prasad & Moon, 2022; Tonhauser & Ristvej, 2019; Tsao et al., 2022).

As is known, information security is normatively defined in the Doctrine of information security of the Russian Federation[5]. In compliance with this document, "information security is a condition of protection of a personality, society, and the state against internal and external information threats, ensuring implementation of constitutional rights and freedoms of a person and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity and sustainable social-economic development of the Russian Federation, defense and safety of the state"[6].

The task of ensuring information security, including through effective control over the activity of communication operators, is rather comprehensible to the extent that implies the absence of the need to specially justify it. All communication operators in Russia constitute a single communication network in the state and ensure integrity, accessibility, and in certain cases confidentiality of data, sustainability and security of information-communication infrastructure as a whole. As was justly noted by A. K. Zharova, the Internet, the general purpose networks, and the local networks functioning on the territory of the Russian Federation, though not being state information systems, provide access to the information contained in state information systems. Accordingly, the security of functioning of such technologies and access channels must be ensured by legal tools (Zharova, 2022).

National security is no longer determined solely by a military component and the state borders. Cyber threats are of sporadic and multidimensional character, creating risks of colossal harm. At that, these threats cannot be prevented by solely traditional means, such as military force or law enforcement mechanism; they require effective bilateral cooperation between governments and the private sector (Li & Liu, 2021).

---

4 See, for example: Kalmykov, D. A. (2005). *Information security: notion, position in the criminal legislation of the Russian Federation, problems of legal protection*: thesis for a Candidate Degree in Jurisprudence. Yaroslavl. https://elibrary.ru/nnomvb; Kubyshkin, A. V. (2002). International-legal problems of ensuring the information security of a state: thesis for a Candidate Degree in Jurisprudence. Moscow; Lopatin, V. N. (2000). Information security of Russia: thesis for a Doctoral Degree in Jurisprudence. Saint Petersburg.

5 Order of the President of the Russian Federation No. 646 of 05.12.2016. (2016, December 12). *Collection of legislation of the Russian Federation*, *50*, Article 7074.

6 *Ibid*.

Nevertheless, Russia has for a long time not built the architecture of regulating the public-private interaction in this sphere. Accordingly, the question of liability of communication operators for inobservance of the necessary information security standards was not posed. One cannot say that such decisions were not maturing in the public conscience and were not being discussed as promising in the professional community. Discussion was held rather actively, but, as often happens, direct implementation required the changed social conditions and the formation of an actual demand in terms of providing state security.

It is easy to understand why the respective changes in the Russian criminal legislation regarding the liability for violations in using TMCT appeared at the present stage. Recently, cyber attacks on the information infrastructure have increased exponentially (Elchaninova, 2020; Truntsevsky, 2019; Krasinsky & Mashko, 2023; Bokshitskii & Meltseva, 2017), including during the COVID-19 pandemic (Lallie et al., 2021; Hoheisel et al., 2023; Khisamova & Begishev, 2022). Besides, they are of a complex character, testifying to the thorough preparation of such actions, presence of high competencies and costly equipment of the wrongdoers (Horsman, 2021; Kouloufakos, 2023; Boughton, 2019). Roskomnadzor refers to it in its comments about the legislative innovations under study. In particular, they specially marked that "under a hybrid war, including elements of information confrontation and regular cyber attacks, protection of the information space of Russia is critically important for the state and society. In this regard, communication operators must unconditionally comply with the requirements to installation, exploitation and modernization of TMCT and requirement to pass all traffic through them. All technical means for counteracting threats are under control of the Center for monitoring and management of the general purpose communication network (further – CMM GPCN), which ensures counteracting information attacks"[7].

Another relevant circumstance is that, under the growing international tension and information confrontation, of utmost significance is the observance of the introduced restrictions in access to certain network resources. In other words, it was necessary not only to bring the information flow under technological control (filtration) and build barriers preventing citizens' access to certain traffic and mobile applications, but also effectively ensure liability of communication operators for evading from following these standards. Roskomnadzor also explained as follows: "Operators often pass traffic beyond TMCT or for one reason or another allow switching off this equipment. This may threaten the stable functioning of the Internet in Russia and lead to a failure in the work of information resources of state bodies. If TMCT are switched off or traffic is passed beyond them, Russian users get access to dangerous information: children's pornography, pro-drug content, propaganda of suicide, fakes, extremist information"[8].

---

7 Roskomnadzor states that operators' refusing to use TMCT threatens citizens. (2022, July 15). https://tass.ru/obschestvo/15228891

8 *Ibid*.

Decision on building a monitoring system using TMCT generally complies with the provisions of the Doctrine of information security of the Russian Federation, which defines the following main directions of its implementation: counteraction against using information technologies for propaganda of extremist ideology, dissemination of xenophobia, ideas of national exclusiveness with a view of undermining sovereignty, political and social stability, violent alteration of constitutional order, violation of territorial integrity of the Russian Federation; disruption of the activity inflicting harm to the national security of the Russian Federation, performed using technical means and information technologies by special services and organizations of foreign states and individuals, etc.

It is important to note that the measures on regulating relations associated with TMCT introduction, taken at the national level, largely comply with the trends of foreign countries (Bitzer et al., 2023; Cascavilla et al., 2021; Mohamed, 2013; Nguyen & Golman, 2021; Broadhead, 2018; Qamar et al., 2023). In this article, we do not pursue the goal of giving a detailed estimation to the processes taking place globally. At the same time, it is necessary to form a general idea of them, in order to better understand the situation with TMCT functioning in Russia.

In a certain sense, the Russian model of regulating and protecting the relations associated with introduction and use of TMCT repeats the experience of the People's Republic of China (further – PRC). As is justly marked in literature, billions of Internet users in PRC gave the state great economic advantages, but it also creates real threats to its economic and political security (Dremliuga et al., 2017). China was one of the first to face the risks and estimate the "benefits" emerging in case of nonintervention into the activity of telecommunication operators at the national level (Ye & Zhao, 2023). Today, many popular foreign Internet resources are blocked in PRC because they disseminate information contradicting the ideology of China and moral attitudes of the society, have signs of terroristic or extremist propaganda. Moreover, a PRC Law of on security of the Internet of 2016[9] obliges providers demand from the users to register under their real names, filter the content and implement blocking the resources, use only certified equipment, follow the requirement to localize users data, provide technical support and assistance to the bodies of public and state safety, etc. Violating of the respective rules providing the safety of the PRC network space may lead to forcible termination of the activity of the communication operator, as well as bringing their employees to liability, including criminal one.

In the Russian literature it is justly stated that the repressive Chinese legislation in the Internet sphere, besides violation of the rights and freedoms apparent for the western

[9] *In China, a headline-making Law on cyber security is coming into force*. https://ria.ru/20170601/1495523455.html

community, also seriously contribute to the "filtration" of the illegal content occurring in the Chinese segment, thus protecting statehood and citizens against terrorism, extremism, cults, pornography, violence, attacks of foreign intelligence services, etc. (Luzyanin & Troshchinsky, 2018).

Within the Commonwealth of Independent States (further – CIS), the approach associated with determining liability for violating the rules of using TMCT is not widely spread. The Agreement on cooperation of the CIS member states in struggling against crimes in the sphere of information technologies[10] also lacks respective recommendations. Probably the closest in meaning are the provisions of Article 2781 "Violation of informatization rules" of the Criminal Code of the Republic of Uzbekistan[11].

On December 20, 2018, the EU Directive 2018/1972 of 11.12.2018 of the European Parliament and of the Council establishing the European Electronic Communications Code[12] came into force. According to it, the member states must provide that suppliers of public electronic communication networks or public electronic communication services take due and proportionate technical and organizational measures for proper management of risks associated with the safety of the networks and services. Given the level of technology, these measures must ensure the level of safety corresponding to the current risks. European Union Agency for Cybersecurity (ENISA) is intended to coordinate activities of member states to avoid discrepancies in national requirements, which might create the risks to security and barriers for the internal market. The member states also must ensure that the suppliers of public electronic communication networks or public electronic communication services notify, without unjustified delays, an authority body of a security incident which had significantly influenced the functioning of the networks and services.

Member states must ensure that authority bodies are entitled to issue mandatory guidelines, including referring to the measures necessary to eliminate a security incident or prevent its occurrence, to the suppliers of public electronic communication networks or public electronic communication services. Member states must ensure that competent bodies are entitled to demand from the suppliers of public electronic communication networks or public electronic communication services: to provide the information necessary to estimate the safety of their networks and services, including documented safety policies; to be subject to safety audit, carried out by a qualified independent body or a competent body, and submit its results to a competent body; the audit is paid for by the supplier[13].

---

10 Agreement on cooperation of member states of the Commonwealth of Independent States in struggling against crimes in the sphere of information technologies. (2022, August 15). *Collection of legislation of the Russian Federation*, *33*, Article 5883

11 https://lex.uz/docs/111457#111470

12 *Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02018L1972-20181217

13 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L1972#d1e4938-36-1

The Directive determined the changes in legislation of EU states on telecommunication technologies and data protection. For example, on April 22, 2021, Germany adopted the Telecommunications Modernization Act (TKMG). Also, Telecommunications Telemedia Data Protection Act (TTDSG) was adopted – the law on data protection in telecommunications in Germany, accompanied by a new technical regulation on implementing the legal measures for monitoring of telecommunications. The new requirements to the security of telecommunications sector introduce a category of "critical components of telecommunications". These components may be used only if they are tested and certified by an officially recognized certification body and if the component producer submitted to the communication operator a "reliability declaration". In compliance with the new regulatory regime, operators with the increased potential risk must use relevant intrusion detection systems (IDS) and/or attack detection systems (ADS). Also, such operators must undergo external security audit every two years[14].

On November 17, 2021, Great Britain adopted the Telecommunications (Security) Act 2021[15]. This law introduced changes in the Communications Act of 2003.[16] Among the most significant provisions is the direct definition in Article 105A of obligation of communication operators to identify threats to cyber resilience and take steps to overcome and prevent them. Also, Article 105B stipulates the obligation of communication operators to execute the instructions of a state regulator. Article 105E stipulates that a state controlling body possesses authorities to prepare and adopt the rules of providing cyber resilience. The respective rules stipulating technical standards and specific practices of security are obligatory for providers. The functions of immediate control and supervision over executing the rules are imposed on the Office of Communications (OFCOM).

Violation of rules and standards of telecommunication security, evading the instructions of OFCOM entails significant fines, including turnover-based ones. Article 404 of the British Communications Act stipulates the issue of the probable brining to criminal liability of a company head, "if the deed is committed by a legal person and it is proved that it was committed with the consent or with the connivance of, or was associated with any negligence on the part of a director, a manager, a secretary or another person executing managerial functions".

On June 14, 2022, discussion of Bill C-26 was initiated in Canada, aimed at making amendments in the Communications Act[17]. Its aim is to promote the state security and to ensure cyber resilience of the telecommunication infrastructure by giving the respective state structures new authorities regarding control over the activities

14 https://www.gesetze-im-internet.de/ttdsg/

15 https://www.legislation.gov.uk/ukpga/2021/31/contents/enacted

16 https://www.legislation.gov.uk/ukpga/2003/21/contents

17 https://www.parl.ca/legisinfo/en/bill/44-1/C-26

of communication operators. Examining the draft law allows making a conclusion that the list of such authorities is very large and implies not only surveillance over the observance of the stipulated security standards, but also the possibility to impose prohibitions on using certain equipment, to provide communication services to certain users, etc. Notably, the draft law caused active discussions. For example, an open letter to the Minister of public safety was published, stating that "Bill C-26 empowers the government to secretly order telecom providers "to do anything or refrain from doing anything". This opens the door to imposing surveillance obligations on private companies, and to other risks such as weakened encryption standards – something the public has long rejected as inconsistent with our privacy rights"[18]. Professional community claimed a substantial and unjustified restriction of the freedom of economic activity, as well as the fact that the proposed standards would ruin small participants of the telecommunications services market. The bill was not adopted so far.

Thus, if we try to define the direction of development of the foreign legislation on telecommunications in the most general terms, one may make a conclusion that it consists of an attempt to build a system of public-private interaction, in which communication operators would perceive the problem of information security not as their internal task, but as an element of the overall state security. In this regard, it is easy to trace the statement of the need for effective control over the activity of communication operators, first of all in the sphere of the introduced technical standards of providing cyber resilience.

3. Regulation in the sphere of centralized management of technical means of counteracting the threats to information security

The obligation of a communication operator rendering services of access to information-telecommunication network Internet to ensure installation of TMCT in their network is stipulated by clause 5.1 of Article 46 of Federal Law of July 7, 2003, No. 126-FZ "On communication"[19]. The respective provision for the first time appeared in the Russian legislation with the adoption of Federal Law of May 1, 2019, No. 90-FZ "On making amendments in the Federal Law 'On communication' and Federal Law 'On information, information technologies and protection of information'"[20].

It is important to note that the legislative initiative appeared as a response to the USA National Cyber Strategy adopted in September 2018. As was stated in the explanatory memorandum to the law draft, "the document signed by the US President declares the principle of 'forcible peace maintenance'. At the same time, Russia is explicitly and groundlessly accused of committing hacker attacks; punishment is explicitly mentioned: "Russia, Iran,

18 https://ccla.org/privacy/joint-letter-of-concern-regarding-bill-c-26/

19 (2003, July 14). *Collection of legislation of the Russian Federation*, *28*, Article 2895.

20 http://publication.pravo.gov.ru/Document/View/0001201905010025

and North Korea conducted reckless cyber attacks that harmed American and international businesses and our allies and partners without paying costs likely to deter future cyber aggression". Under these conditions, protective measures are necessary to provide long-term and sustainable functioning of the Internet in Russia and to increase the reliability of the Russian Internet resources. The necessary rules of traffic routing are determined; control over their implementation is organized. Possibility is created to minimize data transfer abroad, exchanged by the Russian users. Trans-border communication lines and traffic exchange points are determined. Possibility is implied to install technical means on communication networks to identify the source of the traffic transferred. The technical means would be able to limit access to resources with prohibited information not only by network addresses but also by prohibiting the transfer of the traffic passed"[21].

The Law of May 1, 2019 No. 90-FZ, also known as the Law "On sovereign Runet", caused fundamental disputes and even protests among some representatives of the industry and civil society. It was noted that its implementation creates unjustified risks to constitutional rights and freedoms of citizens, will require billions of costs, threaten competition in the communication services market, and will facilitate corrupt behavior[22]. This situation is largely similar to the one around discussing Bill C-26 in Canada, which was mentioned before. Nowadays, one may definitely say that there was no other possible solution for Russia. Undoubtedly, creation of a single contour of information infrastructure protection in the state requires significant funding. One also has to agree with the thesis of a cardinal broadening of state control over citizens' activity in the virtual environment. At the same time, the balance is important, which determines the state of information security as a dynamic system changing under the influence of external conditions.

The main document currently determining the regulation in the sphere of managing the technical means of ensuring cyber resilience of digital networks is the Decree of the Government of the Russian Federation of February 12, 2020 No. 126 "On installation, exploitation, and modernization in the communication networks of a communication operator of the technical means of counteracting the threats to sustainability, safety and integrity of functioning on the territory of the Russian Federation of information-telecommunication network Internet and general purpose communication network"[23].

Analysis of this legal act allows concluding that the mechanism of interaction between radio frequency service and a communications operator is of multistage character. The rules stipulate that not later than 90 calendar days before the planned date TMCT

---

21 Explanatory memorandum "To the draft of Federal Law 'On making amendments to certain legislative acts of the Russian Federation'". *SPS KonsultantPlyus*.

22 See: Business critiqued the details of transiting to a 'sovereign Runet'". (2019, June 26). *Kommersant*. https://www.kommersant.ru/doc/4012730?ysclid=ldkccj43i272099969; Head of RSPP stated corruption risks of the Law on 'sovereign Runet'". (2019, July 30). RBK. https://www.rbc.ru/technology_and_media/30/07/2019/5d3f08389a7947ada3baf05b

23 (2020, February 24). *Collection of legislation of the Russian Federation*, *8*, Article 1001.

installation, a communications operator is sent an inquiry to submit information including: patterns of building the network of the communications operator; technical characteristics of the communication means of the communications operator; locations of the planned installation of TMCT; number of data transfer channels with indication of physical properties of such channels, their technology and carrying capacity; information on average and maximal load of channels; information on the node structure at the location of the planned installation of TMCT; information of the plans of modernization, reconstruction of the communication node, liquidation of a fragment of communication network; technical information and technological parameters of communication means of the communications operator, necessary for the development of project documentation on installation and connection of TMCT.

A communications operator is obliged to prepare an answer to the relevant inquiry within 15 working days after receiving it. The decree stipulates the possibility of sending a clarification inquiry during seven working days after receiving the answer. In that case, the communications operator must prepare an answer within three working days after receiving it.

In general, this procedure of information exchange is intended to ensure the necessary preparation for implementing the coordinated plan for installation and/or modernization of TMCT. From the criminal-legal viewpoint, of interest is the qualification of the actions of communications operator's officials who purposefully evade from submitting the relevant information or knowingly submit incorrect data. We assume that, in the presence of factual evidences, one should consider the possibility to apply Article 201 CC RF and 327 CC RF, respectively. While the situation is rather unambiguous in case of using a knowingly fake document, in case of authority abuse it is necessary to establish not only inaction of the person but also occurrence of negative consequences, for example, a large-scale failure in the functioning of information-communication facilities, etc. At that, it is important and, apparently, difficult for implementing the criminal liability mechanism to establish the cause-effect connection between the evasion of submitting data, absence of TMCT at specific communication channels, and the actual dangerous consequences.

Of great importance for applying the provisions of administrative and criminal legislation is clause 10 of the Rules, which stipulates the obligations of communications operator when exploiting technical means for counteracting threats: to supply electric energy to TMCT; to provide technical support of TMCT functioning in terms of switching them to their communications network, organizing a technological channel for controlling these means, including in compliance with the technical conditions of the TMCT installation; to provide, not later than 48 hours from the moment of occurrence of a requirement from the Radio Frequency Service, an access to TMCT by representatives of the Radio Frequency Service; not to bar the Radio Frequency Service to conduct remote control of TMCT using special software; to observe the requirement to providing the functioning of TMCT, stipulated by exploitation documentation; to provide execution of a complex of measures aimed at safe exploitation of TMCT, including those implying the exclusion of hardware, software and physical impact of unauthorized persons on the TMCT functioning, etc.

Analysis of the above provisions of the Rules allows concluding that, in some cases, bringing the representatives of communications operator to liability will imply the need to directly indicate the violation of specific provisions and requirements stipulated by other documents (for example, an instruction on interaction of the authorized persons of communications operator with the Radio Frequency Service, equipment, etc.).

The technical conditions of installation, as well as the requirements to networks when using TMCT, are stipulated by the Order of Roskomnadzor of July 31, 2019 No. 228 "On adopting the technical conditions of installation of technical means for counteracting threats, as well as requirements to communication networks when using the technical means for counteracting threats"[24].

In addition, one should mention that regulation in terms of TMCT management is not limited to the cited normative acts and is currently characterized as numerous, multilevel and, accordingly, predictably complex. Among such regulation one should specifically mention: Decree of the Government of the Russian Federation of November 3, 2022 No. 1978 "On adopting requirements to the system of ensuring observance by communications operators, rendering communication services and services of passing traffic in the general purpose communications network, of requirements and Rules of functioning and interaction of the system of ensuring observance by communications operators of requirements when rendering communication services and services of passing traffic in the general purpose communications network with information systems and other systems, including with the systems of communications operators"[25], Order of the Russian Ministry of Communications of October 7, 2019 No. 572 "On adopting requirements to ensuring the functioning of traffic exchange points, including the requirements to ensuring the stable functioning of technical and software means of communication, communication facilities, and the order of observing the requirements stipulated by clause 4 of Article 56.2 of the Federal Law of July 7, 2003 No. 126-FZ "On communication"[26], etc.

4. Criminal liability for violating the centralized management of technical means of counteracting the threats to information security

One has to assume that an object of crime stipulated by Article 274.2 CC RF is the public relations associated with exploitation of TMCT and provision of sustainability, security and integrity of functioning in the territory of the Russian Federation of information-telecommunication network Internet and general purpose communication network. Occurrence of these relations between the state and communications operators, as was shown above, has taken place rather recently and had relevant social-legal prerequisites.

24 http://publication.pravo.gov.ru/Document/View/0001201909120028

25 (2022, November 14). *Collection of legislation of the Russian Federation*, *46*, Article 7995.

26 https://minjust.consultant.ru/documents/45269

Of interest is the approach according to which, under the modern condition, an object of crime in the sphere of computer information is public relations in the sphere of digital economy and information society (Dremliuga, 2022). In a certain sense one may agree with this interpretation, based on strategic documents in the sphere of digital economy development. Assumingly, its only drawback is the obvious broadness of the terminology used, which under certain circumstances does not allow identifying the specificity of the given group of publicly dangerous infringements with the special part of CC RF.

The object is the technical means for counteracting threats (TMCT). It is worth noting that there is no list of the relevant equipment in open access. According to the clarifications of the Radio Frequency Service, information about this equipment is a commercial secret.

Part 1 of Article 274.2 CC RF stipulates liability for violating the order of installation, exploitation and modernization in the communication network of technical means for counteracting threats to the stable functioning of the Internet and general purpose communication network, or inobservance of technical conditions of their installation or requirements for their use. Disposition is a blanket one and refers to the Decree of the Government of the Russian Federation of February 12, 2020 No. 126[27].

The objective part of this crime implies both active and passive behavior of a subject and may consist in impeding the distant control of the Radio Frequency Service over the technical means for counteracting threats; violation of requirements contained in exploitation documentation; switching off the technical means for counteracting threats from energy supply; blocking access to the relevant equipment by representatives of the Radio Frequency Service, etc.

According to Part 2 of Article 274.2 CC RF, the objective part consists in passing the traffic via the technical means for counteracting threats. The respective requirements are stipulated by the Order of the Ministry of Digitalization of the Russian Federation of January 26, 2022 No. 44 "On adopting the Requirements to the order of passing the in data transfer networks"[28].

In compliance with the Decree of the Government of the Russian Federation of February 12, 2020 No. 127 "On adopting the Rules of centralized control over the general purpose network"[29], a communication operator is entitled not to route the traffic via the technical means for counteracting threats in the following cases: a) violation of the functioning of the technical means for counteracting threats, when the passage of traffic via the given technical means is terminated, provided the requirements to exploitation of technical means for counteracting threats are observed; b) violation of the functioning of a technical means for counteracting threats, when the parameters of the traffic passage do not correspond

---

27 Decree of the Government of the Russian Federation No. 126 of 12.02.2020. *Collection of legislation of the Russian Federation*, *8*, Article 1001.

28 http://publication.pravo.gov.ru/Document/View/0001202203010002

29 (2020, February 24). *Collection of legislation of the Russian Federation*, *8*, Article 1002.

to the parameters indicated in the project documentation for the installation and functioning of the technical means for counteracting threats, provided the requirements to exploitation of technical means for counteracting threats are observed; c) identification of information or information resources, access to which is not to be restricted in compliance with the legislation of the Russian Federation. Passage of traffic beyond the technical means for counteracting threats in other cases, not stipulated by the Decree No. 127, may be qualified as violation of requirements to the passage of traffic by implication of part 2 of Article 274.2 CC RF.

Both bodies of evidences are constructed using administrative preclusion and imply that the respective violation of rules must be committed during the period when a person is considered subject to administrative punishment for law breaches stipulated by qualification types of Article 13.42 of the Code on Administrative Breaches of the Russian Federation[30] (further – CAB RF) and 13.421 CAB RF. An aggravating element in both cases is the repeatability of the administrative breach of law. Thus, by implication of Article 274.2 CC RF, the signs of a criminally punishable act will only occur after the third violation of the rules of centralized TMCT control.

From the view point of a legislative description, the deed stipulated by Article 274.2 CC RF refers to a numerous group of crimes associated with the violation of special rules, the dual nature of which, in apt words by N. I. Pikurov, are characterized by a combination of an offense and a crime (a "juridical Russian doll" format) (Pikurov, 2009).

The proposed legislative model of liability of the representatives of communications operators for violations in the sphere of TMCT exploitation does not seem optimal. First, rather doubtful is the approach to description of the administratively preclusive signs of the body of evidence. Despite the significance of the relations provided by the system of TMCT centralized control, the possibility of criminal-legal reaction to a particular incident appears not in connection with the occurrence of specific publicly dangerous consequences and even not in case of a traditional repetition, but only after the third documented violation.

In continuation of this idea, one should assume that a legislator has wrongly rejected the model of criminalization of violating TMCT control as a function of inflicting substantial harm to the rights and legal interests of citizens or organizations, or to the legally protected interests of the society or state. In a certain sense, this even now poses the question of qualification of the actions of a representative of a communications operator, who, using their managerial authorities, interfered into the TMCT functioning, which resulted in publicly dangerous consequences (for example, a cyberattack led to the loss of personal data of several thousand users, an information infrastructure of large economic subjects was destroyed, large sums of money were stolen, etc.). We believe that in the presence of the signs of a special subject stipulated by Article 201 CC RF, application of this norm should

[30] (2002, January 7). *Collection of legislation of the Russian Federation*, *1* (part I), Article 1.

be prioritized. This, in particular, is indicated by the coordination of sanctions in the Article 274.2 CC RF and 201 CC RF.

The subject of both crimes is special – an official, as formulated in the note to Article 274.2 CC RF, that is, a person temporary, permanently or by a special authority executing managerial, organizational-administrational or administrative-economic functions in a commercial or other organization, or an individual entrepreneur, subjected to administrative punishment for the respective deeds stipulated by the Code on Administrative Breaches of the Russian Federation.

In the norm under study, a legislator commits a rather not appropriate terminology. They call "officials" the subjects possessing managerial functions in a commercial or another organization (see note to Article 201 CC RF). Thus, two types of officials are stipulated – in commercial or other organizations, as well as in state bodies, local self-government bodies, etc. (see note to Article 285 CC RF).

The subjective part is not directly disclosed in Article 274.2 CC RF. Taking into attention the formal construction of the bodies of evidences, one should conclude that the subjective part of the violation of special rules, by implication of part 1 of Article 274.2 CC RF, and violation of the requirements to traffic passage according to part 2 of Article 274.2 CC RF are expressed by guilt in the form of direct intention. At that, the content of motives and goals does not influence the qualification of crime.

If the respective violations were committed by negligence, due to recklessness in observing exploitation requirements and other rules, the deeds committed, depending upon the circumstances, can be qualified in accordance to Article 274 CC RF or part 3 of Article 2741 CC RF.

Conclusion

In conclusion, one should highlight once again that the decision on creating a closed contour of information protection in Russia by introducing TMCT and building a respective system of relations between the state and communications operators can only be welcomed. Essentially, it does not matter which external or internal causes facilitated the implementation of reforms in the sphere of telecommunications. It is rather wrong to imply that the "sovereign Runet" is a specifically Russian idea, the extraordinary reaction to extraordinary circumstances. It was promoted by much more complex and in-depth processes. This is confirmed by the experience of some foreign countries which either have implemented the respective reforms or are actively moving in that direction.

At the same time, the model of criminal-legal provision of relations in the sphere of TMCT centralized control, stipulated by Article 274.2 CC RF, can hardly be assumed free from drawbacks and contradictions. This is not only the continuation of a rather disputable direction of development of the Russian criminal legislation, associated with broadening the bodies with administrative preclusion in the Special part of CC RF, although this approach has largely excluded the very possibility to differentiate liability for this crime.

The problem is in the very condition of preliminary repeated bringing to administrative liability for the respective deed twice during a year. Rather disputable is also the decision to use the category of an official, to which a legislator has attributed its own "autonomous" meaning exclusively in Article 274.2 CC RF.

The relevance and quality of the norm will very soon be verified by practice. In this respect, one should only rely on time. As for the doctrine, it should traditionally hope for the best and be prepared for the worst, discussing and developing the possible prospective steps to change the law and overcome the problems of law enforcement.

References

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Bokshitskii, V., & Meltseva, I. (2017). Improving the protection of socially significant information resources. *Voprosy Kiberbezopasnosti*, *S2*(20), 11–14. (In Russ.).

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *2019*(4), 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Dremliuga, R. I. (2022). *Criminal-legal protection of digital economy and information society against cybercriminal infringements: doctrine, law, law enforcement*: monograph. Moscow: Yurlitinform. (In Russ.).

Dremliuga, R. I., Korobeev, A. I., & Fedorov, A. V. (2017). Cyberterrorism in China: Criminal Law and Criminological Aspects. *Russian Journal of Criminology*, *11*(3), 607–614. (In Russ.). https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Efremova, M. A. (2018). *Criminal-legal protection of information security*: monograph. Moscow: Yurlitinform. (In Russ.).

Elchaninova, N. B. (2020). Protection of critical information infrastructure as a new institute of legally enforcing information security. *Information Society*, *2*, 58–65. (In Russ.).

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Khisamova, Z. I., & Begishev, I. R. (2022). Digital crime in the context of a pandemic: main trends. *Russian Journal of Criminology*, *16*(2), 185–198. (In Russ.). https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Krasinsky, V. V., & Mashko, V. (2023). Cyberterrorism: criminological characteristics and qualification. *State and Law*, *1*, 79–91. (In Russ.). https://doi.org/10.31857/S102694520024122-5

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends

and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Luzyanin, S. G., & Troshchinsky, P. V. (2018). Ensuring China's national security at the present stage (normative and legal aspect). *Journal of Foreign Legislation and Comparative Law*, *1*, 60–69. (In Russ.). https://doi.org/10.12737/art.2018.1.8

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Pikurov, N. I. (2009). *Qualification of crimes with blanket characteristics of the components of crime*: monograph. Moscow: Russian State Academy of Justice. (In Russ.).

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Truntsevsky, Yu. V. (2019). Unlawful impact on critical information infrastructure: the criminal liability of its owners and operators. *Journal of Russian Law*, *5*(269), 99–106. (In Russ.). https://doi.org/10.12737/art_2019_5_9

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. *Discourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Zharova, A. K. (2022).The legal regulation of relations in the sphere of prevention of possible information technology vulnerabilities. *Bezopasnost biznesa*, *1*, 19–26. (In Russ.). https://doi.org/10.18572/2072-3644-2022-1-19-26

Author information

Evgeniy A. Russkevich – Doctor of Juridical Sciences, Associate Professor, Professor of the Department of Criminal Law, Kutafin Moscow State Law University
Address: 9 Sadovaya-Kudrinskaya Str., 125993 Moscow, Russian Federation
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was performed as part of a state order «Russian legal system under the realities of digital transformation of the society and state: adaptation and prospects of reacting to the modern challenges and threats (FSMW-2023-0006)». Registration number: 1022040700002-6-5.5.1.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 6, 2023
Date of approval – April 13, 2023
Date of acceptance – August 15, 2023
Date of online placement – August 20, 2023

Научная статья
УДК 34:343.3/.7:004:654.1
EDN: https://elibrary.ru/fiseet
DOI: https://doi.org/10.21202/jdtl.2023.28

Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности

Евгений Александрович Русскевич

Московский государственный юридический университет имени О. Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Ключевые слова

Законодательство,
Интернет,
информационная безопасность,
киберпреступление,
киберустойчивость,
оператор связи,
право,
сеть связи,
уголовная ответственность,
цифровые технологии

Аннотация

Цель: получение нового знания об ответственности за нарушение правил управления техническими средствами противодействия угрозам информационной безопасности, разработка теоретических рекомендаций и предложений по совершенствованию законодательства и правоприменения.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе абстрактно-логический, догматический, сравнения и др.

Результаты: на основе изучения документов, изданий сделаны следующие выводы: 1) предпринятые на национальном уровне меры по регулированию отношений, связанных с внедрением технических средств противодействия угрозам, в целом соответствуют положениям Доктрины информационной безопасности Российской Федерации; 2) одним из основных направлений развития зарубежного законодательства о телекоммуникациях является построение системы государственно-частного взаимодействия, при котором операторы связи стали бы воспринимать проблему информационной безопасности не как их внутреннюю задачу, а как элемент общей безопасности государства. В этом отношении предельно четко прослеживается констатация необходимости эффективного контроля за деятельностью операторов связи, прежде всего в сфере вводимых технических стандартов обеспечения киберустойчивости; 3) регулирование отношений в сфере управления техническими средствами противодействия угрозам в России характеризуется многочисленностью, многоуровневостью и, соответственно, вполне

предсказуемой сложностью; 4) реализованная в ст. 274.2 Уголовного кодекса Российской Федерации модель ответственности представителей операторов связи за нарушения в области эксплуатации технических средств противодействия угрозам не представляется оптимальной. Довольно уязвимым является подход к описанию административно преюдициальных признаков состава. Несмотря на значимость отношений, возможность уголовно-правовой реакции на конкретный инцидент возникает не в связи с наступлением тех или иных общественно опасных последствий и даже не при традиционной повторности, а лишь при третьем задокументированном нарушении. Более предпочтительной представляется модель криминализации нарушения управления техническими средствами противодействия угрозам в зависимости от причинения существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства.

Научная новизна: во многом определяется фактической неразработанностью вопросов, связанных с законодательным определением и реализацией уголовной ответственности за нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования.

Практическая значимость: основные положения и выводы исследования могут быть использованы для совершенствования механизма уголовно-правовой охраны информационной безопасности, дальнейшего развития отечественной доктрины уголовного права об ответственности за преступления в сфере компьютерной информации.

Для цитирования

Русскевич, Е. А. (2023). Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности. *Journal of Digital Technologies and Law*, *1*(3), 650–672. https://doi.org/10.21202/jdtl.2023.28

Список литературы

Бокшицкий, В. И., Мельцева, И. С. (2017). Совершенствование защиты общественно значимых информационных ресурсов. *Вопросы кибербезопасности*, *S2*(20), 11–14. https://www.elibrary.ru/zvzggl

Дремлюга, Р. И. (2022). *Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/hsbxrm

Дремлюга, Р. И., Коробеев, А. И., Федоров, А. В. (2017). Кибертерроризм в Китае: уголовно-правовые и криминологические аспекты. *Всероссийский криминологический журнал*, *11*(3), 607–614. EDN: https://www.elibrary.ru/zhnbdp. DOI: https://doi.org/10.17150/2500-4255.2017.11(3).607-614

Ельчанинова, Н. Б. (2020). Защита критической информационной инфраструктуры как новый институт правового обеспечения информационной безопасности. *Информационное общество*, *2*, 58–65.

Ефремова, М. А. (2018). *Уголовно-правовая охрана информационной безопасности*: монография. Москва: Юрлитинформ. https://www.elibrary.ru/zihcgl

Жарова, А. К. (2022). Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях. *Безопасность бизнеса*, *1*, 19–26. EDN: https://www.elibrary.ru/mnaski. DOI: https://doi.org/10.18572/2072-3644-2022-1-19-26

Красинский, В. В., Машко, В. В. (2023). Кибертерроризм: криминологическая характеристика и квалификация. *Государство и право*, *1*, 79–91. EDN: https://www.elibrary.ru/omupsq. DOI: https://doi.org/10.31857/S102694520024122-5

Лузянин, С. Г., Трощинский, П. В. (2018). Обеспечение национальной безопасности Китая на современном этапе (нормативно-правовой аспект). *Журнал зарубежного законодательства и сравнительного правоведения*, *1*, 60–69. EDN: https://www.elibrary.ru/yshope. DOI: https://doi.org/10.12737/art.2018.1.8

Пикуров, Н. И. (2009). *Квалификация преступлений с бланкетными признаками состава*: монография. Москва: Российская академия правосудия.

Трунцевский, Ю. В. (2019). Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов. *Журнал российского права*, *5*(269), 99–106. EDN: https://www.elibrary.ru/krnlwx. DOI: https://doi.org/10.12737/art_2019_5_9

Хисамова, З. И., Бегишев И. Р. (2022). Цифровая преступность в условиях пандемии: основные тренды. *Всероссийский криминологический журнал*, *16*(2), 185–198. https://doi.org/10.17150/2500-4255.2022.16(2).185-198

Bitzer, M., Häckel, B., Leuthe, D., Ott, J., Stahl, B., & Strobel, J. (2023). Managing the Inevitable – A Maturity Model to Establish Incident Response Management Capabilities. *Computers & Security*, *125*, 103050. https://doi.org/10.1016/j.cose.2022.103050

Boughton, N. (2019). Protecting infrastructure from cyber attack. *Network Security*, *4*, 18–19. https://doi.org/10.1016/S1353-4858(19)30051-0

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law & Security Review*, *34*(6), 1180–1196. https://doi.org/10.1016/j.clsr.2018.08.005

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, *105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Colding, J., Colding, M., & Barthel, S. (2020). Applying seven resilience principles on the Vision of the Digital City. *Cities*, *103*, 102761. https://doi.org/10.1016/j.cities.2020.102761

Espinoza-Zelaya, C., & Moon, Y. B. (2022). Resilience Enhancing Mechanisms for Cyber-Manufacturing Systems against Cyber-Attacks. *IFAC-PapersOnLine*, *55*(10), 2252–2257. https://doi.org/10.1016/j.ifacol.2022.10.043

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Hoheisel, R., Van Capelleveen, G., Sarmah, D. K., & Hartel, P. H. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security*, *128*, 103158. https://doi.org/10.1016/j.cose.2023.103158

Horsman, G. (2021). Digital evidence and the crime scene. *Sci. Justice*, *61* (6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kouloufakos, T. (2023). Untangling the cyber norm to protect critical infrastructures. *Computer Law & Security Review*, *49*, 105809. https://doi.org/10.1016/j.clsr.2023.105809

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. *Computer Law & Security Review*, *29*(1), 66–76. https://doi.org/10.1016/j.clsr.2012.11.005

Nguyen, C. L., & Golman, W. (2021). Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. *Computer Law & Security Review*, *40*, 105521. https://doi.org/10.1016/j.clsr.2020.105521

Prasad, R., & Moon, Y. (2022). Architecture for Preventing and Detecting Cyber Attacks in Cyber-Manufacturing System. *IFAC-PapersOnLine*, *55*(10), 2246–2251. https://doi.org/10.1016/j.ifacol.2022.10.042

Qamar, S., Anwar, Z., & Afzal, M. (2023). A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, *128*, 103127. https://doi.org/10.1016/j.cose.2023.103127

Tonhauser, M., & Ristvej, J. (2019). Disruptive acts in cyberspace, steps to improve cyber resilience at National Level. *Transportation Research Procedia*, *40*, 1591–1596. https://doi.org/10.1016/j.trpro.2019.07.220

Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894. https://doi.org/10.1016/j.adhoc.2022.102894

Ye, W., & Zhao, L. (2023). "I know it's sensitive": Internet censorship, recoding, and the sensitive word culture in China. D*iscourse, Context & Media*, *51*, 100666. https://doi.org/10.1016/j.dcm.2022.100666

Сведения об авторе

Русскевич Евгений Александрович – доктор юридических наук, доцент, профессор кафедры уголовного права, Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)
Адрес: 125993, Российская Федерация, г. Москва, ул. Садовая-Кудринская, 9
E-mail: russkevich@mail.ru
ORCID ID: https://orcid.org/0000-0003-4587-8258
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57919310600
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/2510065
Google Scholar ID: https://scholar.google.ru/citations?user=rwKPImIAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=539093

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование выполнено в рамках государственного задания «Российская правовая система в реалиях цифровой трансформации общества и государства: адаптация и перспективы реагирования на современные вызовы и угрозы (FSMW-2023-0006)». Регистрационный номер: 1022040700002-6-5.5.1.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 6 февраля 2023 г.
Дата одобрения после рецензирования – 13 апреля 2023 г.
Дата принятия к опубликованию – 15 августа 2023 г.
Дата онлайн-размещения – 20 августа 2023 г.