DOI 10.52468/2542-1514.2025.9(3).114-123

CYBERSECURITY: CONCEPT, STRUCTURE, THE MECHANISM OF LEGAL ENSURING**

Alexander B. Smushkin
Saratov State Law Academy, Saratov, Russia

Article info
Received –
2024 July 1
Accepted –
2025 June 20
Available online –
2025 September 20

Keywords
Security, cybersecurity, cyberspace, cyber threats, information sovereignty, critical information infrastructure, cybersecurity forensics, digital criminalistics, ensuring the stability of cyberspace, digital technologies, cyber incident

Taking into account the attention paid by the head of state, legislators and law enforcement practitioners to information security, it is necessary to systematically investigate the category of "cybersecurity" as one of its subspecies.

The article undertakes a multifactorial analysis of cybersecurity issues in modern conditions. Special attention is paid to the development of issues of forensic cybersecurity as an important element of countering criminal cyber incidents.

The article is based on the use of materialistic dialectics as a universal method, as well as general scientific methods such as methods of analysis, synthesis, modeling, and extrapolation. Legal methods were also used - comparative legal, formal legal, technical legal.

It is argued that the concept and content of cybersecurity is derived from the general category of "security". The differentiation of cybersecurity and information security has been made. The author identifies the emergent properties of cybersecurity.

Much attention is paid to the elements of cybersecurity, the subjects and objects of this state, as well as the main categories of cybersecurity. The specific scope of application of cybersecurity measures (incident cyberspace) leads to the emergence of specific technological security facilities. Such objects include critical information infrastructure, software and databases of organizations, information technology devices of users, Internet of Things (IoT) devices. Among the most common cyber threats, the author includes: malicious software (viruses, malware, etc.), phishing and social engineering, MITM (Man-in-the-middle) attacks - embedding into the system and intercepting traffic, denial of service attacks (DOS and DDOS-attacks), data leaks and privacy violations. Cybersecurity actors include users themselves, the state, law enforcement agencies and specialized non-governmental organizations for countering cyber threats - Group IB, Kaspersky Lab, developers of software complexes aimed at protecting in cyberspace, etc. Each cybersecurity subject has a certain set of rights and obligations. A range of unresolved issues has been identified and some ways of solving them have been outlined. The article also focuses on the issues of legal regulation of cybersecurity in Russia.

The author states that cybersecurity in modern conditions is a complex multilevel system, ensuring optimal functioning of which can be achieved only by complex, systematic measures that give a synergistic effect. At the same time, the forensic aspects of cybersecurity must necessarily be proactive, defining technical, tactical and methodological issues of forensic cybersecurity.

** The research was carried out at the expense of the Russian Science Foundation grant No. 24-28-00312, https://rscf.ru/project/24-28-00312/.

ISSN 2658-4050 (Online)

1. Introduction

Information security was set by the President of the Russian Federation as a task necessary to achieve the national goal "Digital transformation of state and municipal administration, economy and social sphere"[1]. The high attention paid to this area is also emphasized by the adoption in 2016 of the Information Security Doctrine of the Russian Federation[2], reflecting the system of official views on ensuring the national security of the Russian Federation in the information sphere.

A subspecies of information security (along with physical information security, endpoint security, data encryption, etc.) is cyber security [1, p. 46]. The great attention paid by the country's leader to this issue urgently requires the development of the concept, structure, subjects and the very essence of this category.

Cybersecurity, as an element of general information security, is primarily related to ensuring security against cybercrimes and incidents in cyberspace that are not criminalized. The need to identify a separate category of cybersecurity in science and practice is due to the steady increase in the number of cybercrimes and the increase in damage from them. For example, Russian Interior Minister Vladimir Kolokoltsev reported at a meeting of the Interior Ministry board dedicated to countering IT crimes that "Since 2020, the number of attacks using information technology has increased by a third. The share of remote acts in the total array is now approaching 40%. ...In total, for 2023 and 4 months of the current year, it [the damage] exceeded 210 billion rubles. ...new ways of committing such attacks are constantly emerging "[3]. It should be noted that the IT crimes highlighted by the leadership of the Ministry of Internal Affairs in statistical indicators (crimes committed using information and telecommunication technologies or in the field of computer information) practically correspond to the crimes highlighted in the Budapest Convention on Cybercrimes (Computer Crimes)[4]. According to the UN recommendations, "cybercrime" is any crime that can be committed using a computer system or network, within a computer system or network, or against a computer system or network" [5]. In English, the prefix "Cyber" is defined as related to information technology[6].

[1] Paragraph "l" of Part 8 of Decree of the President of the Russian Federation dated 05/07/2024 N 309 "On the National Development Goals of the Russian Federation for the period up to 2030 and for the future up to 2036". Official website of the President of the Russian Federation URL: http://www.kremlin.ru/events/president/news/63728 (accessed 05/27/2024)

[2] Decree of the President of the Russian Federation No. 646 dated December 5, 2016 "On Approval of the Information Security Doctrine of the Russian Federation". Collection of Legislation of the Russian Federation No. 50 dated December 12, 2016, art. 7074

[3] Vladimir Kolokoltsev held a meeting of the Board of the Ministry of Internal Affairs of Russia dedicated to combating IT crime. Official website of the Ministry of Internal Affairs of the Russian Federation https://мвд.рф/news/item/51089163 (accessed 11.06.2024)

[4] Convention on Computer Information Crime ETS N 185 (Budapest, November 23, 2001). Garant URL: https://base .garant.ru/4089723/?ysclid=m2so62hc1u539532568 (accessed 29.10.2024)

[5] Report of the Xth United Nations Congress on the Prevention of Crime and the Treatment of Offenders/ Makarevich, I. I. The practice of translating terms of international law in terms of the implementation of the UN Sustainable Development Goals. BSU, 2015. P. 2

[6] Cambridge Explanatory Dictionary URL: https://dictionary.cambridge.org/ru/словарь/англо-русский/cyber , free. - (accessed 10/25/2024).

ISSN 2542-1514 (Print)

Many scientists interpret cybercrime precisely as "crime related to both the use of computers and the use of information technology and global networks."" [2; 3; 4;5], or, similarly to M.A. Prostoserdov, "information and telecommunication networks and the cyberspace formed by them [6, p. 30]. These factors suggest that the terms "IT blunting" and "Cybercrime" are considered synonymous for the criminalistic purposes of countering cybercrime and ensuring cybersecurity. The need to develop measures to counter these threats leads to increased relevance, including forensic support.

Some aspects of information security have been studied in the works of such Russian authors as I.V. Kubyshkin, I.L. Bachilo, A.A. Streltsov, I.A. Polyakov, G.G. Gorshenkov, V.N. Lopatin, L.V. Bogomolova, A.A. Baranova, V.A. Kopylov, P.U. Kuznetsov, E.A. Krasnenkova, N.N. Kunyaev, T.A. Polyakova, and others.

Cybersecurity issues were considered in the works of domestic and foreign authors, such as: Stepanov-Egiyants, V. G., Meshcheryakov V.A., Stelmakh A.P., Tonkonogov A.V., Vekhov V.B., Gribanov D.V., Dremlyuga R.I., Kuchin Ya.O., Begishev I.R., Jafarli V.F., Wang Xiao Ling (Wang, XiaoLing), Kelemen Miroslav, Szao Stanislav, Vajdova Iveta (Kelemen, Miroslav & Szabo, Stanislav & Vajdova, Iveta), John D. Howard, J. C. Smith, W. Fayyad, G. Pyatetsky-Shapiro (Fayyad, U., Piatetsky-Shapiro, G.), Wilson K. (Wilson. K.) and others. However, due to the rapid development of electronic technology, information technology devices, the emergence of new forms of information (for example, distributed information, etc.), new types of threats (for example, polymorphic viruses, quantum technologies aimed at hacking identification and authentication systems), these works, while maintaining their methodological importance in Currently, they are already lagging somewhat behind the development of cybersecurity threats and counteraction methods.

With the beginning of a special military operation, crime in cyberspace has received a new incentive and vector of development, becoming almost a threat to national security, which necessitates the development of cyber security issues.

2. The concept of security

The category "cybersecurity" is derived from the general definition of security (naturally, taking into account the specific cybernetic sphere of the application). Security is a multifaceted concept, however, it is mainly defined as the state of an object (for example, "the state of protection of transport infrastructure and transportation facilities from acts of unlawful interference") [7]. A similar approach can be seen in other regulations[8].

In the information sphere, the legislator proceeds from the fact that security is a state of security: "the security of a critical information infrastructure is a state of security of a critical information infrastructure, ensuring its stable functioning during computer attacks against it." We also consider it necessary to use a legislative

[7] Federal Law No. 16-FZ of February 9, 2007 "On Transport Safety". Collection of legislation of the Russian Federation dated February 12, 2007, No. 7, art. 837

[8] Federal Law No. 116-FZ of July 21, 1997 "On Industrial Safety of Hazardous Production Facilities". Collection of Legislation of the Russian Federation No. 30 of July 28, 1997, art. 3588; Federal Law No. 7-FZ of 01/10/2002 "On Environmental Protection" (as amended by 08.08.2024)// Collection of Legislation of the Russian Federation dated January 14, 2002, No. 2, Article 133; Decree of the President of the Russian Federation dated December 31, 2015, No. 683 "On the National Security Strategy of the Russian Federation". Collection of Legislation of the Russian Federation, 2016, No. 1, Article 212, etc.

ISSN 2658-4050 (Online)

approach[9].

M.A. Efremova points out that "security in a broad sense should be considered both statically as a state of security, and dynamically as a set of measures taken to ensure this state" [7, p.56]. It seems to us that the static and dynamic elements named by her must be considered simultaneously, in synergy, since the "state of security" in itself, if it is not explained by objective measures, will be absurd. Therefore, taking into account the definition of M.A. In particular, security can be understood as a state of security caused by a set of measures aimed at preventing the occurrence of threats and their suppression.

Depending on the structural level, security can be personal, public (of the whole society or individual collectives), state and international. Differentiation can also be carried out depending on the sphere of vital activity, the type of threats, etc.,

the following signs (properties) of security can be conditionally distinguished:

- absence or blocking of threats;

-the possibility of stable and sustainable development;

-availability and sufficiency of a system of hazard prevention measures;

- availability of a system of risk forecasting measures;

- availability of assistance;

- the existence of strict rules and procedures for ensuring safety;

- access control and management.

However, it should be noted that security at each of its structural levels and in each sphere of life acquires individual, characteristic emergent features..

[9] Federal Law No. 187-FZ of July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation". Collection of Legislation of the Russian Federation dated July 31, 2017 N 31 (part I) art. 4736

3. The concept and essence of cybersecurity

The concept of "Information security" used in the domestic legal field is not completely identical to the one under consideration. Cybersecurity is a state of security not from any information threats, but only from digital threats in cyberspace and not from any threats, but only from cyber threats [8].

In our opinion, one of the most successful definitions of cyberspace is proposed in the Model Law of the CIS member states on Countering Cybercrime: "cyberspace is a digital environment resulting from the interaction of people, software and services in information and telecommunications networks, including the Internet, through related technological devices and a family that does not exist in physical form"[10].

The main emergent properties of cybersecurity, in our opinion, are:

• Network connectivity of devices exposed to cyber attacks;

• Encroachment on information in digital form only;

• Technological complexity of information devices exposed to cyber attacks;

• Permanently changing the cybersecurity landscape;

• Data mining and mutual integration of various cybersecurity measures as a prerequisite;

• Flexibility and adaptability of cybersecurity systems;

• Active multi-level protection;

• Focusing not only on repelling attacks

[10] The Model Law on Countering Cybercrime" (Adopted on 04/14/2023 in St. Petersburg by Resolution 55-20 at the 55th plenary session of the Interparliamentary Assembly of the CIS Member States)// Information Bulletin. Interparliamentary Assembly of the Member States of the Commonwealth of Independent States. 2023. N 78 (part 3).

ISSN 2542-1514 (Print)

and suppressing security incidents, but also, to a large extent, on risk management;

• Global reach- most cyber attacks are now cross-border in nature.

Thus, the following scheme of differentiation of cybersecurity and information security can be given:

Differences in purpose (for information security, the goal is to protect information from any threats, for cybersecurity, it is to protect only digital information from cyber threats);

Differences in coverage (within the framework of information security, protective measures are developed for any information, while cybersecurity protects information located in computer networks, systems and databases),

Differences in protective measures (information security is characterized by physical, technical, administrative and other measures, while cybersecurity is characterized by technological and programmatic measures and tools).

The possibility of using the "Digital Security" category should also be considered. It seems to us that since, in relation to information, the adjective digital is used to describe a method of discrete transmission of information, it would be more logical to use the term "Digital information security" (as a separate type of information. However, taking into account the concepts that have been actively used recently, containing the definition of "digital", in the context of using digital (electronic) devices or considering these devices as objects of research ("Digital economy", "Digital forensics", "Digital literacy", etc.), we believe thatI believe that the category "Digital Security" can be used as an analogue of the category "Cybersecurity".

Even using the category "cybersecurity", most documents do not reveal its essence. Moreover, in some cases, the document, having the category "Cybersecurity" in its title, does not disclose it, does not mention it at all in the text (for example: Interstate standard GOST ISO/IEC 27014-2021 "Information Technologies. Information security, cybersecurity, and privacy protection. Management of information security activities")[11].

The Model Law of the CIS member States on countering Cybercrime contains the following definition of cybersecurity: "preservation of confidentiality, integrity and accessibility of information in cyberspace, as well as the security of information infrastructure"[12]. It seems to us that this definition is quite possible to use.

4. Cybersecurity framework

In order to determine the structure of cybersecurity in modern conditions, it is necessary, first of all, to analyze scientific approaches to the elements of security.

V.L. Manilov names the following elements of security: "threats, interests, factors of influence on them and methods of ensuring" [9, p. 17]. According to A.I. Stakhov, the elements of security include: "subjects of security, objects of security, threats of security" [10, p. 6;]. Other authors offer similar interpretations of the structure [11, p.20; 12, p. 6]

[11] Interstate standard GOST ISO/IEC 27014-2021 "Information technologies. Information security, cybersecurity, and privacy protection. Management of information security activities" (put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated July 2, 2021 No. 613-st). Moscow: Standartinform. 2021

[12] The Model Law on Countering Cybercrime" (Adopted on 04/14/2023 in St. Petersburg by Resolution 55-20 at the 55th plenary session of the Interparliamentary Assembly of the CIS Member States)// Information Bulletin. Interparliamentary Assembly of the Member States of the Commonwealth of Independent States. 2023. N 78 (part 3).

Based on the analysis of the opinions of various authors, it can be stated that the cybersecurity structure includes: cybersecurity facilities, cyber threats, and cybersecurity actors.

The specific scope of cybersecurity measures (incident cyberspace) leads to the emergence of specific technological security facilities. Such objects include critical information infrastructure, software and databases of organizations, information technology devices of users, Internet of Things (IOT) devices.

The most important objects include the critical information infrastructure, as defined by the legislator, these are "objects of critical information infrastructure, as well as telecommunication networks used to organize the interaction of such objects"[13]. It is the objects of critical information infrastructure that are, first of all, the focus of attention of the Russian approach to cybersecurity (see, for example, [13]).

Databases of organizations that are subject to cybersecurity breaches can be either open or restricted in nature. At the same time, we consider it necessary to include in these databases and software not only the objects of commercial and non-commercial "private" legal entities, but also the databases and software of state and municipal bodies that are not part of the complex of critical information infrastructure.

Cybersecurity of information technology devices is primarily related to their use as a network element, or the security of the networks themselves as information technology devices. As for computer networks as an object of cyber security, they should be differentiated into several levels: a Body area network, a personal area network (PAN), a local area network (LAN), a campus network (Campus area network-CAN), an urban network (Megapolis area network (MAN) and wide area network (WAN). Interference with the functioning of any level of networks can have serious consequences, from the death of a wearable network carrier due to an untimely response of a stimulant or an insulin pump to the impossibility of international information exchange.

The term "Internet of Things" was coined by Kevin Ashton in 1999. As we have already noted, "Elements of the Internet of Things concept can be used to commit crimes when hacking various systems (when hacking access control and management systems- violation of the inviolability of the home, theft; video surveillance systems- violation of privacy; hacking banking applications or payment applications- theft, etc.), and bear direct or indirect signs of crimes committed by their owners" [14, pp. 455-456]. The importance of studying the cyber security of Internet of Things systems is also emphasized by foreign authors [15; 16]

V.A. Artamonov and E.V. Artamonova are of the opinion that "Cyber threats are a set of conditions and factors under which private and public security is violated, and information danger is created. From the objective point of view, cyber threats are actions taken by criminals in the digital space" [17].

According to Kambulov D.A., the main sources of cyber threats include: "National states; Terrorist organizations; Criminal groups; Hackers; Harmful insiders" [18, pp. 1657-1658].

According to O.G. Kovalev and N.V. According to Semenova, "The main subjects of cyber security at present are officials of state bodies and local governments with appropriate

[13] Parts 6 and 7 of art. 2 of Federal Law No. 187-FZ dated July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation". Collection of legislation of the Russian Federation dated July 31, 2017 N 31 (part I) art. 4736

ISSN 2542-1514 (Print)

powers, among which law enforcement agencies stand out, as well as special services (the Prosecutor General's Office, the Ministry of Internal Affairs, the Investigative Committee, the Federal Security Service, the Ministry of Defense, the Federal Security Service, The Ministry of Justice of the Russian Federation and the Federal Penitentiary Service subordinate to it, as well as the Russian Guard)" [19, p. 13]. It seems to us that the subjects of cybersecurity should be interpreted somewhat more broadly and include users themselves, the state, law enforcement agencies and specialized non-governmental organizations for countering cyber threats - Group IB, Kaspersky Lab, developers of software systems aimed at protection in cyberspace, etc. Cybersecurity actors are primarily those who provide it, and not just those who deal with the consequences of violating it.. Cybersecurity entities have a certain set of rights and obligations related to the possession or use of an information resource, provided for by Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection"[14], as well as the rights provided for by the Code of Criminal Procedure of the Russian Federation, when participating in criminal proceedings in as specialists.

5. Cybersecurity mechanism

We believe that, in essence, the cybersecurity mechanism is a set of strategies, methods and measures aimed at protecting information systems, networks and data in incident cyberspace from various cyber threats. The use of these mechanisms helps to prevent, detect and respond to security incidents.

Among the general methods that make up the cybersecurity mechanism available to any user are: timely installation of updates and fixes, identification and authentication of users, installation and timely use of firewalls and antivirus software.

M.M. Bezkorovayny and A.L. Tatuzov identify, in addition to general methods of ensuring cyberspace security, as well as a group of special methods and a group of intellectual methods

They include special methods for ensuring cyberspace security:

"- analysis of the topological structure and development of recommendations for its modification, methods and specific algorithms for their implementation;

- new methods of cryptographic protection based not only on purely computational mechanisms for implementing resilience, but also on taking advantage of a multi-connected communications architecture and a large number of respectable users;

- information security methods based on social services to counter cyber attacks using special group behavior analysis procedures" [20, p.26].

In intelligent methods, they include:

"- methods of intelligent user identification;

- preventing virus and other attacks;

- detection of attacks and infiltrations;

- situational analysis of the state of information security;

- new methods of cryptographic protection based on neural network technologies" [20, p.26].

One can agree with this approach, however, organizational and criminalistic methods should also be added to the range of methods, considering organizational management, technical and tactical-criminalistic cybersecurity support, and involvement of

[14] Federal Law No. 149-FZ of July 27, 2006 "On Information, Information Technologies and Information Protection". Collection of legislation of the Russian Federation dated July 31, 2006 N 31 (part I) art. 3448

societies of practitioners in the field of cybersecurity.

Organizational measures can also include monitoring and forecasting risks, developing risk mitigation strategies, and training employees in cyber hygiene, understanding and responding to cyber threats.

The main measures to ensure cybersecurity include: strong complex passwords, two-factor authentication; regular account verification; timely updating of security software; monitoring network activity; training and self-education; regular backups; data encryption; security when shopping online and visiting suspicious sites; caution when using public Wi-FiFi networks; development of the use of access restriction and access control strategies; verification of used electronic media; cooperation with organizations established to counteract and investigate computer incidents.

Cybersecurity strategies in foreign countries contain different, but in many ways similar approaches: the use of rapid response forces to computer incidents, the maximum dissemination of information about positive practices against intruders, the responsibility of network operators for insufficient use of security measures, lack of information to relevant structures, etc., special conditions for storing and using users' personal data and others, which allows us to analyze and borrow successful practices for use in our country. .

In the strategic plan, the cybersecurity mechanism includes access control as the first level of countering cyber incidents; a level of system protection, including the necessary software; incident prevention and protection of information systems; risk analysis for systems and networks of various levels; detection, suppression and other response to computer incidents; investigation committed cybercrimes and other cyber incidents. In many ways, cyber security also includes technological sovereignty, reduced dependence on vendors, and the use of domestic software.

It is the Cybersecurity Strategy of the Russian Federation that is urgently needed as a single conceptual document. We can agree with M.A. Prostoserdov that it should include: protection of strategic and government facilities (energy, oil, gas and military-industrial complex, housing and communal services, etc.); ensuring the security of citizens, organizations and the state, both in the field of computer information and in the field of economic relations (property relations and relations in the sphere of economic activity); improvement of legislation; fight against anonymity; international cooperation; development of special law enforcement agencies; development of information technologies; improvement of digital literacy of the population [6, p.178].

6. Conclusions

To summarize, it can be stated that, despite large-scale developments in the field of cyberspace security, digital hygiene and rapid response to computer incidents, many issues in the field of cybersecurity of critical information infrastructure, as well as legal entities and citizens in cyberspace have not been resolved. There is no comprehensive approach to addressing cybersecurity issues of critical information infrastructure involving all entities provided for in paragraph 8 of art. 2 of the Federal Law "On the security of the critical information infrastructure of the Russian Federation", despite the adoption of this law. Critical information infrastructure has a complex architecture, which complicates its protection and increases the complexity of managing cyber risks. To a large extent, this is also facilitated by the insufficient amount of specialized training for law enforcement officials in the field under consideration. Software vulnerabilities persist.

ISSN 2542-1514 (Print)

The intensification of cyber threats during the sanctions war and the special military operation leads to massive attacks on the information resources of Russian authorities. So, at the time of writing this article, the websites of the GAS "Justice", the Judicial Department and the courts on the domain have been inaccessible for almost a month as a result of a hacker attack. sudrf.ru . Limited access to advanced technologies also reduces the security of critical information infrastructure.

Given the cross-border nature of many cyber incidents, it can be noted that only domestic security measures in cyberspace may not always be effective enough. It is necessary to organize international cooperation in this field.

Insufficient software and technological sovereignty has a negative impact on cyberspace security. The use of software systems developed abroad can lead to attacks, information leaks, and control interception through backdoors (back door - "backdoor", literally "back door") - defects in the program algorithm intentionally embedded in it by the developer for subsequent unauthorized access or control interception.

Thus, cybersecurity in modern conditions is a state of cyberspace security of the subject's electronic devices, due to a complex multilevel system, ensuring the optimal functioning of which can be achieved only through comprehensive, systematic measures that give a synergetic effect.

REFERENCES

1. Bogomolova L.V. Information security: what is it in modern realities. *Vestnik nauki i obrazovaniya*, 2023, no. 1-1 (132), pp. 45–48. (In Russ.).

2. Serieva M.M. Cybercrime as a new criminal threat. *Novyi yuridicheskii vestnik*, 2017, no. 1, pp. 104–106. (In Russ.).

3. Nomokonov V.A., Tropina T.L. Cybercrime as a new criminal threat. *Kriminologiya: vchera, segodnya, zavtra*, 2012, no. 1 (24), pp. 45–55. (In Russ.).

4. Nemov M.V. Cybercrime as a new criminal threat. *Epokha nauki*, 2017, no. 9, pp. 47–51. (In Russ.).

5. Alpeev A. Terminology of security: cybersecurity, information security. *Voprosy kiberbezopasnosti*, 2014, no. 5, pp. 39–42. (In Russ.).

6. Prostoserdov M.A. *Economic crimes committed in cyberspace and measures to counteract them*, Cand. Diss. Thesis. Moscow, 2016. 232 p. (In Russ.).

7. Efremova M.A. *Criminal law protection of information security*, Doct. Diss. Moscow, 2017. 427 p. (In Russ.).

8. Balandin A.Y. Cyber security and information security. Demarcation of legal categories. *Pravovaya politika i pravovaya zhizn'*, 2023, no. 3, pp. 260–270. DOI: 10.24412/1608-8794-2023-3-260-270. (In Russ.).

9. Manilov V.L. *Theory and practice of the organization of the national security system of Russia*, Doct. Diss. Thesis. Moscow, 1995. 36 p. (In Russ.).

10. Stakhov A.I. Security in the legal system of the Russian Federation. *Bezopasnost' biznesa = Business security*, 2006, no. 1, pp. 2–7. (In Russ.).

11. Avdeev M.A. *Theoretical and legal foundations of ensuring personal and property security of participants in criminal proceedings*, Cand. Diss. Moscow, 2009. 170 p. (In Russ.).

12. Kondrashov B.P. *Public safety and administrative and legal means of ensuring it*. Moscow, Shchit-M Publ., 1998. 296 p. (In Russ.).

13. Mosechkin I.N. Problems of the Criminal Law Protection of Critical Information Infrastructure of the Russian Federation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 1, pp. 22–34. DOI: 10.17150/2500-1442.2023.17(1).22-34. (In Russ.).

14. Smuskin A.B. Some Aspects of Using the Concept of «the Internet of Things» in Crime Counteraction. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 3, pp. 453–460. DOI: 10.17150/2500-4255.2020.14(3).453-460. (In Russ.).

15. Casarosa F. Cybersecurity of Internet of Things in the health sector: Understanding the applicable legal framework. *Computer Law & Security Review*, 2024, vol. 53, art. 105982. DOI: 10.1016/j.clsr.2024.105982.

16. Weber R.H., Studer E. Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review*, 2016, vol. 32, iss. 5, pp. 715–728. DOI: 10.1016/j.clsr.2016.07.002.

17. Takov A.Z. Cybersecurity issues in modern digital systems. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian legislation*, 2023, vol. 16, no. 5, pp. 232–236. (In Russ.).

18. Kambulov D.A. Cyber security threats. *StudNet*, 2021, vol. 4, no. 7, pp. 1657–1658. (In Russ.).

19. Kovalev O.G., Semenova N.V. Cybersecurity in modern Russia: theoretical and organizational and legal aspects. *Stolypinskii vestnik*, 2021, vol. 3, no. 1, available at: https://stolypin-vestnik.ru/wp-content/uploads/2021/02/Kovalev_O_G_Semenova_N_V_Kiberbezopasnost.pdf. (In Russ.).

20. Bezkorovainy M., Tatuzov A. Cybersecurity - approaches to the definition. *Voprosy kiberbezopasnosti*, 2014, no. 1 (2), pp. 22–27. (In Russ.).

INFORMATION ABOUT AUTHOR

Alexander B. Smushkin – Candidate of Law, Associate Professor; Leading Researcher, Project Office of Scientific Programs and Research; Associate Professor, Department of Criminology
Saratov State Law Academy
104, im. N.G. Chernyshevskogo ul., Saratov, 410056, Russia
E-mail: Skif32@yandex.ru

ISSN 2542-1514 (Print)

ORCID: 0000-0003-1619-8325
ResearcherID: AAM-2853-2020
Scopus AuthorID: 57202012484

BIBLIOGRAPHIC DESCRIPTION

Smushkin A.B. Cybersecurity: concept, structure, the mechanism of legal ensuring. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 3, pp. 114–123. DOI: 10.52468/2542-1514.2025.9(3). 114-123. (In Russ.).