
THE LAW ENFORCEMENT BY THE BODIES OF PRELIMINARY INVESTIGATION AND INQUIRY

DOI 10.52468/2542-1514.2025.9(1).122-131



PECULIARITIES OF QUALIFICATION OF CRIMES IN THE FIELD OF COMPUTER INFORMATION AND COUNTERACTION TO THEM**

Irina A. Efremova

Saratov State Law Academy, Saratov, Russia

Article info

Received –

2024 June 04

Accepted –

2025 January 10

Available online –

2025 March 20

Keywords

Crimes, counteraction,
information and
telecommunication networks, the
Internet, crimes in the field of
computer information

The subject of the study is the specifics of the qualification of crimes in the field of computer information and measures to counter them. The purpose of the study is to examine the specifics of the qualification of crimes in the field of computer information and to develop effective measures to counter them. Research methodology. Along with the universal method of cognition, general scientific and private scientific methods were used: first of all, the statistical method, system-structural analysis, analytical research. This made it possible to comprehensively investigate the specifics of the qualification of crimes in the field of computer information and identify measures to counter them. Scientific results of the study. It has been established that recently there has been an increase in crimes committed in the field of computer information and (or) using information and telecommunication networks. In 2023, the share increased from 26.5% to 34.8% compared to the previous year. More than half of such crimes (50.6%) belong to the categories of grave and especially grave. It is determined that criminal liability for crimes committed in the field of computer information is established in Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information", for crimes committed using information and telecommunication networks - in art. 105; 110; 110.1; 110.2; 111; 112; 115; 116; 117; 119; 126; 127; 127.2; 128.1; 133; 137; 151.2; 159.6; 171.2; 185.3; 205.2; 222; 222.1; 228.1; 230; 238.1; 242; 242.1; 242.2; 245; 258.1; 260.1; 280; 280.1; 280.4; 282; 354.1 The Criminal Code of the Russian Federation, containing a qualifying The attribute is an information and telecommunication network. The classification of this feature as qualifying is based on the degree of public danger of the crime. But there is a varying degree of public danger of these acts. In some formations, the commission of a crime using information and telecommunication networks is a qualified type (art. 110, 110.2, 128.1, 151.2, 205.2, 228.1, 230, 242.1, 242.2, 245, 258.1, 260.1, 280, 280.1, 280.4 of the Criminal Code of the Russian Federation), in others – especially qualified (art. 110.1, 133, 137, 222, 222.1, 242 159.6, 171.2, 185.3, 238.1 of the Criminal Code of the Russian Federation). It is noted that this feature raises questions when qualifying, for example, when identifying an organized group that commits criminal acts using information and telecommunications networks, including the Internet; distinguishing from other crimes. As measures to counteract crimes committed in the field of computer information and (or) using information and telecommunication networks, including the Internet, it is proposed: to develop a concept of economic development to overcome poverty; to instill a culture of using digital technologies, to form positive value orientations; to develop a Concept of crime prevention, in which it is necessary to devote a separate section on these criminal acts; develop a national plan to counter these crimes; to increase the equipment of law enforcement agencies; to create specialized units for countering cybercrime in the structure of the Ministry of Internal Affairs of the Russian Federation, etc. Conclusions about the achievement of the purpose of this study. In the conducted research, the problems of qualification of crimes in the field of computer information are identified and counteraction measures are proposed.

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

1. Introduction

The entry of the Russian Federation into the era of the information society has led not only to changes in the economy, politics, and ways of communication, but also in the criminal sphere. Criminals have adopted new information and telecommunication technologies and shifted illegal activities to the online space, in connection with which crime has acquired new characteristics. Recently, there has been an increase in crimes committed in the field of computer information and (or) using information and telecommunication networks. From January to December 2023, 677.0 thousand were registered. the specified acts. The growth rate compared to the previous year was 29.7%. The share increased from 26.5% to 34.8%. More than half of such crimes (50.6%) belong to the categories of grave and especially grave (342.6 thousand were registered, the growth rate is 25.9%)¹. This is not taking into account the high level of latency of these attacks [1, 146; 2, p. 1601], which varies from 80% to 90% [3, p. 37].

The further increase in crimes of this group will be influenced by an increase in the number of Internet users. Today, 66% of households use the Internet, and by 2030 it is planned to increase this figure to 97%. Therefore, effective measures should be developed to counter these crimes, including criminal law measures.

Scientific research will contribute to the development of effective counteraction measures. The work of Russian and foreign researchers [4, p. 66; 5, p. 2517; 6, p. 85] is devoted to the study of the criminal and legal qualification of socially dangerous acts committed in the field of computer information and (or) using information and telecommunication networks, and to countering them, among which V.A. Bessonov can be singled out., B.V. Vekhov, R.I. Dremlyuga, M.A. Efremov, N.V. Letelkin, M.A. Prostoserdov, I.M. Rassolov, E.A. Ruskevich, T.L. Tropin, and others. However, there

is currently no comprehensive study that would be devoted to the criminal assessment of these socially dangerous acts committed in the field of computer information and (or) using information and telecommunication networks, and countering them. Therefore, we will consider the above using, along with the universal method of cognition, general scientific and private scientific research methods: first of all, the statistical method, system-structural analysis, analytical research.

2. Research results and discussions

Criminal liability for crimes committed in the field of computer information is established in Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information", for crimes committed using information and telecommunication networks - in art. 105; 110; 110.1; 110.2; 111; 112; 115; 116; 117; 119; 126; 127; 127.2; 128.1; 133; 137; 151.2; 159.6; 171.2; 185.3; 205.2; 222; 222.1; 228.1; 230; 238.1; 242; 242.1; 242.2; 245; 258.1; 260.1; 280; 280.1; 280.4; 282; 354.1 The Criminal Code of the Russian Federation, containing a qualifying attribute – information- telecommunication network. However, other socially dangerous attacks can be committed through the use of information and telecommunication networks. For example, in Britain, for the first time, rape was committed using an information and telecommunications network. A group of men raped the avatar of this minor, which had a negative emotional and psychological impact on the minor girl². Sodomy was committed in Samara through the use of the Internet information

¹ Characteristics of the state of crime in the Russian Federation for January - December 2023. Official website of the Ministry of Internal Affairs of Russia. URL: <https://мвд.рф/reports/item/47055751> / (date of access: 20.05.2024).

² British police are investigating the first rape in virtual reality. Rossiyskaya gazeta. URL: <https://rg.ru/2024/01/03/policia-britanii-rassleduet-pervoe-iznasilovanie-v-virtualnoj-realnosti.html> (date of request: 27.05.2024).

and telecommunications network³, but this was not reflected in the criminal law assessment of the act. Therefore, it is proposed to supplement Article 63 of the Criminal Code of the Russian Federation with such an aggravating circumstance as the commission of criminal encroachments using mass media transmission of information [7, p. 15] or using information and telecommunication networks [8, p. 10].

This was supported by government agencies, and it was proposed to add Part 1 of Article 63 of the Criminal Code to the aggravating circumstance of public demonstration, including in the media or information and telecommunication networks (including the Internet), and art. 111, 112, 115, 116, 117, 127 The Criminal Code of the Russian Federation qualifies the commission of a crime involving a public demonstration of the process of its implementation using mass media or electronic or information and telecommunication networks (including the Internet)⁴. However, other crimes may be committed through the use of information and telecommunication networks, and therefore the proposed list of crimes is insufficient.

The classification, designated as qualifying criteria, is based on the degree of public danger, which is a quantitative sign of public danger [9, pp. 319-321]. The degree of public danger is based on the nature of the public danger, circumstances mitigating and aggravating punishment, and other factors characterizing a person's willingness to commit a new encroachment on objects of criminal protection. Determining the degree of public danger is the level of readiness of a person to commit a new crime. The state of readiness is

based on the nature of the harm caused to the relevant object of the crime (an objective indicator) and the person's receipt of full or incomplete satisfaction from the encroachment committed by him (a subjective indicator) [10, p. 545]. Crimes committed using information and telecommunication networks encroach on various objects of criminal protection (life, health, public safety, etc.) and the perpetrators do not receive adequate satisfaction from the committed act, which is confirmed by the fact that the criminals have been committing these acts for a long time. E., S., and D. committed theft from bank accounts of various individuals' persons more than one year old⁵.

The duration of the acts analyzed in order to meet their needs is affected by their cross-border nature, causing significant damage and their poor disclosure. In 2023, the detection rate of crimes committed using information and telecommunication networks or in the field of computer information was 26.6%⁶.

But the establishment of a designated qualifying feature in most crimes will cause problems in qualification, since currently many questions arise during criminal law assessment, and therefore the Plenum of the Supreme Court of the Russian Federation has developed and adopted a resolution on judicial practice in criminal cases of computer crimes, as well as other crimes committed with using electronic or information and telecommunication networks, including the Internet. It provides an interpretation of computer information, computer devices, legally protected computer information, computer programs, destruction, blocking, modification, copying, computer information, neutralization of computer information protection tools, unauthorized access to computer information, information and telecommunications network, Internet site; indicates the end of crimes committed

³ Reference on the results of the analysis of judicial practice in the consideration of criminal cases of crimes in the field of computer technology (prepared by the Samara Regional Court on 09.26.2022). URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOPV&n=453462#RmnkXEUKzJNS0WvM1> (date of request: 27.05.2024).

⁴ Letter of the Supreme Court of the Russian Federation dated September 13, 2023 No. 4-VS-4557/23 "Official Response to the Draft Federal Law No. 506240-8 "On Amendments to the Criminal Code of the Russian Federation".

⁵ Criminal case No. 1-54/2019, located in the archive of the Central District Court of Chita, Zabaykalsky Krai.

⁶ Characteristics of the state of crime in the Russian Federation for January - December 2023. // Official website of the Ministry of Internal Affairs of Russia. URL: <https://мвд.рф/reports/item/47055751> / (date of access: 20.05.2024).

in the field of computer information and crimes committed using information and telecommunication networks, including the Internet; the rules for the qualification of these acts, etc. are indicated. But this did not eliminate all the issues that arise in practice. For example, the Supreme Court of the Russian Federation recognized the unjustified qualification of the act under paragraph "b" of Part 2 of Article 228.1 of the Criminal Code. It follows from the materials of the criminal case that for the production and sale of narcotic drugs, the person acquired all the necessary equipment through the Internet information and telecommunications network. With his help, he has been producing narcotic drugs for a long time. But the Supreme Court of the Russian Federation pointed out that the qualifying feature "using information and telecommunication networks (including the Internet)" is used in relation to the sale of narcotic drugs and psychotropic substances⁷. In the case under consideration, no sales were carried out.

Questions also arise when identifying an organized group that commits a crime using information and telecommunications networks, including the Internet. The law enforcement practice in this part varies in the same courts. Incorrect criminal law qualification of the act will entail the imposition of criminal punishment, which will not allow achieving its goals and objectives of the criminal law, and therefore this issue is one of the most urgent today. Thus, the court excluded the qualifying feature – an organized group, reclassifying it to the fact that the act was committed by a group of persons by prior agreement using the Internet information and telecommunications network. It follows from the materials of the criminal case that E., S. and D. committed theft from the bank accounts of individuals. Malware was installed on the victims' phones, which allowed the perpetrators to carry out the theft unhindered. Having excluded the

organized group, the court pointed out that in the course of the investigation, such a feature of it as an association for the commission of a criminal offense was not established, since their association was based not on purposeful activity, but on friendship, as well as such a feature as the stability of the organized group (justifying that the perpetrators could leave it)⁸.

In the process of considering another criminal case, the court agreed with the criminal law assessment of what had been done and recognized that the crime was committed by a completely organized group using the Internet information and telecommunications network. It followed from the materials of the criminal case that the members of the organized group were friends⁹. The territorial dispersion and anonymity of the participants of an organized group committing socially dangerous acts under study also causes problems with qualification, and therefore the preliminary investigation authorities do not establish that the act was committed by an organized group. Consequently, this affects the achievement of the goals of criminal punishment. But unfortunately, scientists do not consider this problem. The explanations of the Plenum of the Supreme Court of the Russian Federation in this part are also missing.

Currently, there are various effects of the considered method of committing a crime on the degree of public danger. In some formations, the commission of a crime using information and telecommunication networks is a qualified type (art. 110, 110.2, 128.1, 151.2, 205.2, 228.1, 230, 242.1, 242.2, 245, 258.1, 260.1, 280, 280.1, 280.4 of the Criminal Code of the Russian Federation), in others – especially qualified (art. 110.1, 133, 137, 222, 222.1, 242 of the Criminal Code of the Russian Federation), thirdly, as a criminalizing feature of the main composition of a criminally punishable act (Articles 159.6, 171.2, 185.3, 238.1 of the Criminal Code of the Russian Federation). The qualified composition

⁷ The Supreme Court indicated a qualifying feature not used in drug production cases. Russian Agency for Legal and Judicial Statistics. URL: <https://rapsinews.ru/publications/20221103/308440464.html> (date of request: 27.05.2024).

⁸ Criminal case No. 1-54/2019, located in the archive of the Central District Court of Chita, Zabaykalsky Krai.

⁹ Criminal case No. 1-949/2018, located in the archive of the Central District Court of Chita, Zabaykalsky Krai.

and the specially qualified composition of the crime differ in the degree of public danger: the level of a person's readiness to commit a new offense and the perpetrator's receiving full or incomplete satisfaction from the act he committed. By virtue of the indicated criteria, the presented can be attributed to a particularly qualified type of composition.

Bringing perpetrators to criminal responsibility and imposing punishment corresponding to the degree and nature of the public danger of the committed act is the implementation of counteraction to socially dangerous acts¹⁰ committed in the field of computer information and (or) using information and telecommunication networks by criminal legal means. But in order to effectively counteract the criminal encroachments under study, a whole range of counteraction measures should be developed.

The term "counteraction" means an action that prevents another action [11, p. 204] directed against it [12, p. 234]. In relation to the legal theory, crime prevention is present when the activities of government agencies, society and individuals are opposed to the activities of committing or preparing to commit socially dangerous attacks [13, p. 159]. Countering socially dangerous acts committed in the field of computer information and (or) using information and telecommunication networks is carried out in two directions: general social (identification and elimination of economic, social, legal, cultural and moral causes and conditions of the crime under study) and special criminological counteraction (identification and elimination of special determinants through prevention (general, individual, victimological) and the suppression of crimes of the group in question). By detecting and influencing the determinants, it is possible to achieve a reduction in these acts.

In order to counteract the analyzed criminal offenses, it is necessary to reduce the level of poverty of the population, since poverty is the locomotive of crime. Persons who commit crimes in

the field of computer information or using information and telecommunication technologies, in most cases, pursue the goal of enriching themselves. Today, many measures are being taken in the country to overcome poverty: for example, monthly payments are being made to full families with low incomes, monthly allowances for children from 3 to 8 years old, two-stage indexation of basic social benefits, etc¹¹. Without delving into the study of these counteraction measures, since they lie in a different plane of research, we would like to point out that it is necessary to develop a concept of economic development to overcome poverty, which would include short- and long-term measures. This will reduce the level of poverty in the Russian Federation and will have a positive impact on reducing the quantitative and qualitative indicators of the studied criminal attacks.

Proper upbringing and education of the younger generation will also have a positive effect on countering the crimes of the group in question. The introduction of a person to the benefits of the digital world begins from childhood. Every day, a child sees how parents and others use various digital technologies, so he gets used to their constant presence. In this regard, children need to instill a culture of using digital technologies and form positive value orientations. It is possible to influence a person's value orientations through upbringing, education, culture [14, p. 37], religion, etc. The combination of these measures can have a positive effect on the value orientations of the individual.

In order to determine the activities of the State to counteract the socially dangerous attacks under study, a Crime Prevention Concept should be developed and adopted, in which it is necessary to devote a separate section to these criminally punishable acts. The concept of crime prevention is the development of a state program that defines the fundamental principles of preventing these crimes, the goals and objectives of the state that will be set to counter them. The concept allows you to define the fundamental foundations of the activity.

¹⁰ This ensures a correct criminal law assessment of what has been done.

¹¹ Expert: support for families with children has helped reduce poverty in Russia. TASS. URL: <https://tass.ru/obschestvo/17240199> (date of request: 23.05.2024).

For its effective implementation, it would be advisable to develop a national plan to counteract the crimes under study, which will contain specific measures that need to be taken to counteract the acts of the analyzed group, since, firstly, they are quite common in the country, and also encroach on various objects of criminal protection, and secondly, they have an increased public danger.

Most of all, scientists propose to increase the equipment of law enforcement agencies conducting preliminary investigations of these acts in order to counteract socially dangerous acts committed in the field of computer information and (or) using information and telecommunications networks. A special place in the structure of information technologies is occupied by "big data" [15, p. 152; 16, p. 7032]. The use of big data technologies can assist in solving various tasks related to the collection of data on criminals, the recording of criminal behavior, connections, the formation of an "electronic personal file"; the control of negative groups. Artificial intelligence will allow predicting criminal behavior based on available data about his personality, the causes and conditions of the crime he committed, the nature of their commission, etc., which will increase the effectiveness of activities to counteract the criminal acts in question [17, p. 763-764; 18, p. 14]. At the same time, digital technologies should be continuously developed that would facilitate the detection and disclosure by law enforcement agencies of criminally punishable acts under study [19, p. 898; 20, p. 681; 21, p. 47; 22, p. 882; 23, p. 845; 24, p. 977; 25, p. 423].

The creation of specialized units for countering cybercrimes in the structure of the Ministry of Internal Affairs of the Russian Federation will have an impact on improving the effectiveness of countering the analyzed acts through their disclosure. This was pointed out by V.A. Kolokoltsev¹², since they are the most common and have features that should be possessed by

persons investigating them. It is also proposed to create the composition of courts dealing with cases involving socially dangerous acts committed in the field of computer information and (or) using information and telecommunication networks¹³.

3. Conclusion

Thus, there is an increase in socially dangerous acts committed in the field of computer information and (or) using information and telecommunication networks. They encroach on various objects of criminal protection (life, health, public safety, etc.) and the perpetrators do not receive adequate satisfaction from the committed act. Therefore, it is necessary to develop effective measures to counteract crimes (for example, such measures include the development of a concept of economic development to overcome poverty, which would include short- and long-term measures; concepts of crime prevention; equipping law enforcement agencies with modern investigative technologies; creation of special departments dealing with the investigation of crimes under study), including criminal law. The latter consists in improving the criminal law and the practice of its application.

¹² Kolokoltsev called for strengthening efforts to counter IT crime and cyber theft. TASS. URL: <https://tass.ru/obschestvo/11943461> (date of request: 27.05.2024).

¹³ Special cybercrime units may be created in the Russian Federation, but not a new court – Supreme Court. [https:// Russian Agency for Legal and Judicial Statistics. URL: rapsinews.ru/judicial_news/20230607/308981899.html](https://RussianAgencyforLegalandJudicialStatistics.rapsinews.ru/judicial_news/20230607/308981899.html) (date of request: 27.05.2024).

REFERENCES

1. Polyakov V.V. Latency of high-tech crimes: concept, structure and methods of assessing its level. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2023, vol. 17, no. 2, pp. 146–155. (In Russ.).
2. Yussuph T.T., Muhammed J.W., Olalekan D.M., Yusuf B., Unuriode A., Matti B.H. Data protection and privacy as a tool to reduce financial loss from cybercrimes. *Global Scientific Journal*, 2023, vol. 11, iss. 11, pp. 1596–1606.
3. Sukharenko A. Modern criminal threats and challenges to information security of Russia. *Protivodeistvie terrorizmu. Problemy XXI veka = Counter-terrorism*, 2012, no. 2, pp. 36–41. (In Russ.).
4. Caneppele S., Aebi M.F. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, 2019, vol. 13, iss. 1, pp. 66–79. DOI: 10.1093/police/pax055.
5. Mmbodi R., Hlongwane N. Cybercrimes in Social Networking. *International Journal of Social Science and Human Research*, 2024, vol. 7, iss. 4, pp. 2517–2522. DOI: 10.47191/ijsshr/v7-i04-38.
6. Aldoghmi H.S. The Role of International Efforts in Combating Cybercrimes. *The International Journal of Humanities & Social Studies*, 2024, vol. 11, iss. 11, pp. 85–92. DOI: 10.24940/theijhss/2023/v11/i11/HS2311-019.
7. Antipov A.I. *Criminal and legal significance of the use of mass media and information and telecommunication networks of the Internet in the commission of crimes with signs of appeals, inducement of illegal trafficking of objects and materials*, Cand. Diss. St. Petersburg, 2022. 248 p. (In Russ.).
8. Shutova A.A. *Criminal law counteraction to information crimes in the field of economic activity: theoretical and applied aspects*, Cand. Diss. Nizhny Novgorod, 2017. 264 p. (In Russ.).
9. Lopashenko N.A. (ed.). *Criminal law. The general part. Crime*, Academic course, in 10 volumes. Moscow, Yurlitinform Publ., 2016. Vol. 3: Criminal policy. Criminal liability. 507 p. (In Russ.).
10. Razgildiyev B.T. Fundamental aspects of criminal punishment. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2017, vol. 11, no. 3, pp. 542–550. (In Russ.).
11. Maiorov A.V. *Victimological model of crime prevention*, Monograph. Moscow, Yurlitinform Publ., 2014. 223 p. (In Russ.).
12. Tupichkina E.A., Semenaka S.I. The influence of socio-cultural factors on the transformation of value orientations of Russian youth. *Nauchno-pedagogicheskoe obozrenie = Pedagogical Review*, 2022, no. 4 (44), pp. 37–47. (In Russ.).
13. Ovchinskii V.S. *Criminology of the digital world*, Textbook. Moscow, Norma Publ., INFRA-M Publ., 2018. 351 p. (In Russ.).
14. Subashka Ramesh S.S., Anshu A., Kumar V., Kumar H. Using Big Data, An Extensible System for Forecasting and Analyzing Relations Among Crimes. *Turkish Journal of Computer and Mathematics Education*, 2021, Vol. 12, no. 10, pp. 7032–7040. DOI: 10.17762/turcomat.v12i10.5577.
15. Sukhodolov A.P., Bychkova A.M. Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2018, vol. 12, no. 6, pp. 753–766.
16. Clifford R. (ed.). *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, 3rd ed. Carolina Academic Press, 2011. 312 p.
17. Kirilenko V.P., Alekseev G.V. The harmonization of Russian criminal legislation on counteracting cybercrime with the legal standards of the Council of Europe. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 898–913. (In Russ.).
18. Osipenko A.L., Solovov V.S. Main trends in the development of criminological theory and crime prevention practice in the context of the digitalization of society. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2021, vol. 15, no. 6, pp. 681–691. (In Russ.).
19. Dremluga R.I., Korobeev A.I. Criminal law policy in counteracting the use of networking platforms for criminal activity. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2022, vol. 16, no. 1, pp. 47–56. (In Russ.).
20. Lantukh E.V., Ishigeev V.S., Gribunov O.P. The use of special knowledge in the investigation of computer crimes. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 882–890. (In Russ.).
21. Mkrtchian S.M. Property crimes in the blockchain sphere: new criminal schemes and their criminal law assessment. *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 6, pp. 845–

22. Vershinina I.A., Liadova A.V. Data in the digital world: New opportunities or additional risks?. *Vestnik Rossiiskogo universiteta družby narodov. Seriya: Sotsiologiya = RUDN Journal of Sociology*, 2020, vol. 20, no. 4, pp. 977–984. DOI: 10.22363/2313-2272-2020-20-4-977-984. (In Russ.).

23. Serebrennikova A.V. Criminological problems of the digital world (digital criminology). *Vserossiiskii kriminologicheskii zhurnal = Russian journal of criminology*, 2020, vol. 14, no. 3, pp. 423–430. (In Russ.).

INFORMATION ABOUT AUTHOR

Irina A. Efremova – Doctor of Law, Associate Professor; Professor, Department of Criminal and Penal Enforcement Law; Professor, Department of Prosecutorial Supervision and Criminology *Saratov State Law Academy*
1, Vol'skaya ul., Saratov, 410056, Russia
E-mail: efremova005@yandex.ru ORCID:
0000-0003-0071-1999
ResearcherID: HJY-8774-2023
RSCI SPIN-code: 3413-7425; AuthorID: 320387

BIBLIOGRAPHIC DESCRIPTION

Efremova I.A. Peculiarities of qualification of crimes in the field of computer information and counteraction to them. *Pravoprimenenie = Law Enforcement Review*, 2025, vol. 9, no. 1, pp. 122–131. DOI: 10.52468/2542-1514.2025.9(1).122-131. (In Russ.).

