Серия «Политология. Религиоведение»
2019. Т. 30. С. 63–74
Онлайн-доступ к журналу:
http://izvestiapolit.isu.ru/ru

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 352/354-1
DOI https://doi.org/10.26516/2073-3380.2019.30.63

The Information Security in the Municipalities of Transbaikal Region of Russia

T. E. Beydina, A. V. Novikova, A. N. Kukharsky

Transbaikal State University, Chita, Russian Federation

Abstract. Information security a direct connection with an increase in both technical and informational means in political relations and the review of the goals and objectives of state and municipal authorities, national, regional and municipal security institutions. The transition to a new level of solving the problems of information security and new tasks of the Russian state and society in modern conditions are related to the emergence of completely new threats to both national security as a whole and its main components – socio-political and information security. These threats need to be addressed, including by introducing new information security systems and the modernization of information communication channels. The problems of Trans-Baikal Territory of Russia, being a depressed region, make this issue highly important. These factors indicate the need to rethink the attitude and develop completely new conceptual approaches to information security issues.

Keywords: Information security, political process, political communication, communication process, national security, managerial communication, e-democracy, political engagement, national authorities, municipal authorities, channels of information, public opinion, public opinion polls in Russia, Transbaikal region.

For citation: Beydina T.E., Novikova A.V., Kukharsky A.N. The Information Security in the Municipalities of Transbaikal Region of Russia. *The Bulletin of Irkutsk State University. Series Political Science and Religion Studies,* 2019, vol. 30, pp. 63-74. https://doi.org/10.26516/2073-3380.2019.30.63

The relevance of the research. Nowadays, as a result of social and economic changes, Russian society has got entirely new conditions which are characterized, in particular, by the coalescence of the bodies of state and municipal authority with business structures. This fact has contributed to setting new priorities and objectives for the bodies of state authority, municipalities and security institutions.

One of the important prerequisites for the social and political development of Russia is keeping low crime rate. At the present time tools and means of combating criminal activities do not entirely comply with conditions and dynamic of organized crime.

The relevance of the study of various information security management tools in a context of integrating information systems is the result of the fact that the problems of information security are commonly viewed from technical standpoints.

Many researchers have pointed out that the problem of information security is limited solely to the computer protection concerns. O. V. Genne pointed out: “Effective implementation of the strategic approach requires coherent consideration of various factors of information security” [5].

The study is aimed at specification of theoretical and legal regulations, methodological principles of municipalities in the TransBaikal region.

In accordance with the intended purpose, the paper offers the following tasks: to study and to clarify theoretical and methodological foundations of the state regulation in the area of information security and organization of such security in municipalities; to define the ways of improvement of legal instruments of information security, management decisions, institutional and legal measures against the information crimes; to analyze the role of institutional and legal mechanisms of information security within the municipal information management systems; to develop proposals for improving information security in municipal authorities.

The object of the research is the information security of Russian municipal bodies. The subject of the research is legal and organizational tools for maintaining information security in municipalities of the Trans-Baikal region.

The study is based on academic papers of Russian and foreign scientists on the reviewed problems in the field of information protection. Theoretical and methodological basis for the study were as follows: V. Arsentiev [2], Yu. M. Baturin [3], N. I. Vetrov [15], V. B. Vekhov [4], B. V. Zdravomyslov [14], A. Krutskyh [9], Yu. I. Lyapunov [10], V. V. Panferov [11], N. N. Potrubach [12], O. G. Sivakov [13], L. Chernyak [16].

Organizational and legal characteristics of information security: theoretical analysis. Organizational and legal measures of ensuring the information security are commonly represented as the set of laws, management decisions, standards which regulate both common activities in ensuring the information security and functions of specialized information security systems. The primary functions of the organizational and legal maintenance of information security are following: elaborating basic principles and methods of classifying confidential information as a protected information; regulating bodies and officials responsible for information security ensuring; developing legal framework which regulates the system of information security; clarifying liabilities for violations of the rules of information security; establishing the order of settlement of conflict and disputable situations on information security issues; establishing tax and economic relations in information era to combat cybercrime effectively and to protect information; improving the mechanisms of tax and economic incentive measures for science and technology in the sphere of information security.

According to S. G. Aksenov, “The basic principles for ensuring the organizational and legal information security are as follows: compliance with the standards and regulations by individuals dealing with protected and confidential information; establishing legal liabilities for violations of the rules and regulations; giving legal force to all technical and mathematical aspects of organizational and legal information security; procedural implementation of resolving situations in ensuring information security” [1].

It should be noted that the legislative framework of any state in the field of information security is the essential measure to satisfy the basic needs for information protection in the development of socio-economic, political and military aspects of the state. Special attention of the western countries to this framework is caused by increasing costs of fighting crime in the field of information. This requires western world to deal seriously with legislative issues in the field of information security.

Thus, in the USA the first law on that issue was enacted in 1960. Nowadays there are more than 500 legislative acts concerning information security, liability for disclosure of this information and computer crime. While forming a legislative framework, the state protects its information resources. Information resources of the state are divided into three groups (figure) [8]:

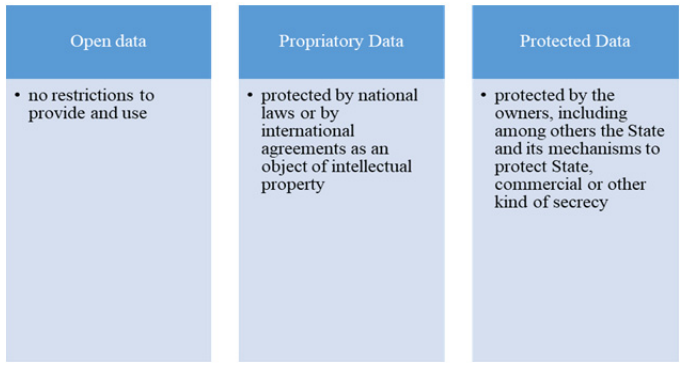

Fig. Kinds of information resources of the state
by A. O. Bezzubtsev, A. N. Kovalev

Protection deals with important data for users. Prohibition on disclosure of significant information facilitates the following tasks: Information that constitutes a state secret is commonly categorized as protected data; Information that constitutes a commercial secret is commonly viewed as confidential data.

The notion of state secret is an important one for the information security. It is the basic element of the information security system in functioning of state authorities. Legislation of the Russian Federation on State Secrets is mainly based on Federal Law "On State Secrets" where "a state secret is the State's protected information in the sphere of its military, foreign policy, economic, intelligence, counter-intelligence and crime detection operations, the spread of which might be prejudicial to the security of the Russian Federation"[1].

The essential elements of information comprising a state secret are following: items and events comprising a state secret; protection of a state secret against enemy; reference to the appropriate item of the list of secret information in Federal Law; the State's protected information in the sphere of its military, foreign policy, economic, intelligence, counter-intelligence and crime detection operations, the spread of which might be prejudicial to the security of the Russian Federation. Information constituting a state secret is regulated by Presidential Decree, November 30, 1995, N 1203.

The principles whereby a secret stamp is not attached to information: declassification of Information does not threaten the safety and violations of the legislation; withholding information will violate the rights of citizens; information might be prejudicial to the health and life of citizens.

[1] О государственной тайне : закон Российской Федерации от 21.07.1993 № 5485–1 (изд. 08.03.2015). URL: http://www.consultant.ru/document/cons_doc_LAW_2481/ (дата обращения: 14.02.2019).

The intelligence shall not be subject to be referred to state secret and be classified is contained in the article 7, Russian Federal Law "On State Secrets". The rules for classification of State secrets are determined in "the Rules of Information Constituting State Secret by Different Levels of Classification"[1]. The degree of damage depends on the degree of secrecy after its disclosure.

Methods of information security are developing in three directions: the individual's right to privacy, the interests of the state and the financial and economic activity. Organizational and legal characteristics of information security involve an analysis of legal and regulatory framework which includes: The Constitution of the Russian Federation, federal laws and laws of the Russian Federation, codes of Russian Federation, government degrees of the Russian Federation, Department regulations, guidance documents, State Standards.

It is worth noting the federal laws and the laws of the Russian Federation regulating relations in information sphere: "On State Secrets", "On security", "On Licensing of Separate Types of Activity", "On Information, Information Technologies and the Protection of Information", "On Communications", "On Commercial Secrecy", "On Electronic Signatures"[2].

Information threats assessment in municipalities. With the development of information society global trends dictate conditions of full information openness of the bodies of state authority. In this connection, standards regulating access of the persons concerned with the information public resources, are being formed. In elaborating management decisions, the state authority is also dependent on the information resources. This is reflected in local self-government (which accumulates and stores operational data), since its work is closely connected with all spheres of human activity: "The rapid advent of the information society, provision of electronic public and municipal services and the development of electronic workflows contributes to the increase of dependence of municipal authorities on used information, its quality, reliability and timeliness" [6].

According to expert opinions numerous databases have been threatened by unauthorized access which causes the negative impact on confidential data thus breaking the principles of information security. Different research papers do not clearly define information security risks in local self-government. This research attempts to define risk factors outlined in "Information Security Doctrine of the Russian Federation"[3]: threats to the constitutional rights and freedoms of man and the citizen in

[1] Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности : распоряжение Правительства РФ от 04.09.1995 № 870. URL: http://www.consultant.ru/document/cons_doc_LAW_7686/ (дата обращения: 12.02.2019).

[2] О безопасности : федер. закон от 28.12.2010 № 390-ФЗ. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=187049; О государственной тайне : закон РФ от 21.07.1993 № 5485-1. URL: http://www.consultant.ru/document/cons_doc_LAW_2481; О связи : федер. закон от 07.07.2003. № 126-ФЗ. URL: http://www.consultant.ru/document/Cons_doc_law_4-3224/; Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности : распоряжение Правительства РФ от 04.09.1995 № 870. URL: http://www.consultant.ru/document/cons_doc_LAW_7686; Об информации, информационных технологиях и защите информации : федер. закон от 27.07.2006 № 149-ФЗ. URL: http://www.consultant.ru/document/-Cons_doc_LAW_61798/; О лицензировании отдельных видов деятельности : федер. закон от 04.05.2011 № 99-ФЗ. URL: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=-LAW;n=113–658; Об электронной подписи : федер. закон от 06.042011 № 63-ФЗ. URL: http://www.consultant.ru/document/ cons_doc_ LAW_112701/ (дата обращения: 14.02.2019).

[3] Об утверждении доктрины информационной безопасности Российской Федерации : указ Президента РФ от 09.09.2000 № 646) // Рос. газ. 2000. 28 сент.

the area of spiritual life and information activities; threats to information support to municipalities; threats to Russian information industry (including informatization, telecommunication, and communication facilities, effective utilization of local information resources); threats to the security of information systems and facilities on the territory of municipality.

Information threats to the constitutional rights and freedoms of man and the citizen in the area of spiritual life and information activities are affected by the following factors: adoption by local bodies of normative legal acts infringing the constitutional rights and freedoms of citizens in the areas of their spiritual life and information activities; establishment of monopolies on forming, receiving and disseminating information with the use of telecommunication systems within the territory of municipality; counteraction, by criminal structures in particular, against citizens' exercise of their constitutional rights to personal and family privacy and to the secrecy of postal mail, telephone and other communications; unlawful restrictions on access to open information resources; illegal use of special means of influence on individual, group and public consciousness; noncompliance by bodies of state authorities of different levels or by organizations and citizens with the requirements of the federal legislation governing relations in the information sphere; unlawful restrictions on access by citizens to open information resources of state authorities of different levels to open archival materials and to other open socially significant information; disorganization or destruction of a system of accumulation and preservation of cultural properties on the territory of municipality; violation of the constitutional rights and freedoms of man and the citizen in the field of mass information; a decrease in the human potential of the population in municipality that would substantially complicate training manpower resources for adoption and use of newest information technologies; information manipulation (disinformation, information concealment and distortion).

The threats endangering information support to Russian Federation state policy may be as follows: monopolization of the Russian information market by a limited number information entities; blocking of activities of state media in providing information both on the territory of a municipality and in the border regions; low level of state policy information support effectiveness due to qualified personnel shortage and the lack of a system of forming and implementing a municipal information policy.

The given paper considers the factors frequently endangering information security. Municipal authorities and officials point to vulnerability of a technical aspect of information systems whether already deployed or being set up on the territory of municipality.

They include: illegal information gathering and use; information processing technology violations; insertion into hardware or software products of components realizing functions not envisaged by documentation for these products; development and distribution of programs that upset the normal functioning of information and information information security systems; destruction, damage, disturbance of, or electronic attack against information processing and telecommunication systems; attacks on password key protection systems for automated information processing and transmission systems; discreditation of cryptographic information protection keys and means; technical channel information leaks; implantation of electronic

intercept devices into information processing, storage and transmission hardware via communication channels; destruction or theft of machine processable data carriers; interception of information in data transmission networks or on communication lines, deciphering of this information; use of uncertified domestic and foreign information technologies, information protection means and informatization; unsanctioned access to information contained in databases; breach of the lawful restrictions on information dissemination [8].

In different levels of authority the sources of threats to the information security are commonly subdivided into external and internal ones. The specific nature of local authorities enables to take into account internal sources whereby it is hard to distinguish external ones since they are closely connected with the inner resources of the country. It is problematic to make a clear distinction between the two parameters. We can suppose that the most significant source is the level of corruption in municipality.

Corruption is closely related to information security since we can observe the existence of organized economic groupings and criminal structures. As a result of access to confidential information, community is increasingly influenced by crime, thus ultimately the interests of the citizens and the interests of the state tend to have lower protection in information sphere. The significant decrease in corruption will be possible if municipal information systems, being limited and controlled, have greater transparency. This requires the establishment of sensitive information management systems for municipality that incurs both financial and staffing challenges. On the one hand, insufficient funding of municipal information security is connected with budgetary norms (companies are funded either when it is necessary or to comply with normative requirements), on the other hand, in order to establish effective security systems, sophisticated technologies are required. When introducing such technologies, a systematic approach should be employed and more funding should be provided. Municipal budgets often fail to implement it whereas lack of systematic principles does not provide effective information protection. The threats endangering information support to municipality are related to economic development and effective territorial governance.

The problems of ensuring the information security in municipalities of Trans-Baikal region from the perspective of authorities. One of the trends of globalization is a cooperative work of different countries on the establishment of global information society. Information society may be defined as a social entity with information as an essential tool and information technologies as a labour instrument. Information relations are largely determined by these circumstances whereas the economy is based on the information products.

Such society represents an association of countries that have achieved growth in economic and social spheres, informatization, scientific development and education. Such rates are extremely essential for the positive economic development and the maintenance of strategic stability in the world. In spite of joining the global information society, countries still have their national interests to be defended. Thus, in establishing the information society, national interests in information are protected.

The Information Security Doctrine of the Russian Federation, approved by Presidential Decree on December 2016, represents basic guidelines for ensuring information security. The Doctrine defines the national interests of the Russian Federation in the information sphere and sets out the guidelines to implement na-

tional interests and to prevent different threats. Nowadays the implementation of Doctrine guidelines is being actively pursued. It is necessary to outline the main ingredients in this area.

The first ingredient of Russia's national interests in the information sphere comprises observance of rights and freedoms of man and the citizen to receive and to use information. Achieving this requires raising information infrastructure usage efficiency for the sake of social development. That principle represents a significant challenge since it is difficult to ensure equal access to advanced information technologies in social inequality. Therefore, the State should provide the establishment of information supportive institutions for a certain part of the population.

It is necessary to improve the principles of streamlining the system of formation and rational utilization of information resources that form the basis of the scientific, technical and spiritual potential of the Russian Federation; to secure the constitutional rights and freedoms of man and the citizen freely to seek, receive, transmit, produce and disseminate information by any legal means. Nevertheless, the right of free access to information should not lead to violation of the constitutional right of man and the citizen to personal and family privacy, the secrecy of postal mail, telegraph, telephone and other communications, as well as to the defense of honor and reputation. Moreover, when guaranteeing the freedom of mass information and the prohibition of censorship, the state should reinforce the mechanisms of legal regulation of relations in the field of intellectual property protection and create conditions for observance of the federally prescribed restrictions on access to confidential information

The following factors and circumstances, regarded as threats in the Doctrine, prevent the successful overcoming the challenges: adoption by federal bodies of state authority of different levels of the Russian Federation of normative legal acts infringing the constitutional rights and freedoms of citizens in the area of information activities; establishment of monopolies on forming, receiving and disseminating information; counteraction, by criminal structures in particular, against citizens' exercise of their constitutional rights to personal and family privacy and to the secrecy of postal mail; illegal use of special means of influence on individual, group and public consciousness; disorganization or destruction of a system of accumulation and preservation of cultural properties; ousting of Russian news agencies and media from the national information market; depreciation of spiritual values, the propaganda of specimens of mass culture; a decrease in the spiritual, moral and creative potential of the Russian population.

The second ingredient includes information ensuring of State policy. This ingredient involves intensifying the formation of open government information resources and bolstering the state mass media, expanding their capabilities to promptly convey reliable information. The main threats in this area include: monopolization of individual sectors or all of the Russian information market by domestic and foreign information entities; blocking of activities of state media in providing information to Russian and foreign audiences; low level of state policy information support effectiveness due to qualified personnel shortage and the lack of a system of forming and implementing a state information policy.

The third ingredient comprises promoting modern information technologies, the national information industry (the industries of informatization, telecommunica-

tion, and communication facilities in particular), securing the satisfaction of domestic market requirements with its products, and their entry into the world market, and providing for accumulation, storage reliability, and effective utilization of national information resources.

Achieving this requires developing the infrastructure of the unified information space of the Russian Federation; developing the Russian information services industry and raising the efficiency in utilization of government information resources; developing the production in the Russian Federation of competitive informatization, telecommunication and communication systems and means, and expanding participation by Russia in the international cooperation of producers of these systems and means.

The fourth ingredient comprises protecting information resources against unsanctioned access, and securing the information of telecommunication systems. For these purposes it is necessary, first of all, to enhance the security of information systems including communication networks, mainly the security of primary communication networks and information systems in the federal bodies of state authority, the bodies of state authority of the constituent entities of the Russian Federation, credit and banking spheres, the sphere of economic activity as well as the security of systems and means for informatizing weapons and military equipment.

The main threats include: activities of foreign, intelligence and criminal elements in illegal collection of information, insertion into hardware or software products of uncertified components that upset the normal functioning of information systems; information processing technology violations; use of uncertified domestic and foreign information technologies, information protection means; breach of the lawful restrictions on information dissemination.

Implementation of measures, which are regarded as primary in the Doctrine, aimed at ensuring information safety in the Russian Federation, is not possible without a thorough and integrated scientific approaches: humanitarian, scientific and personnel ones.

Resolving humanitarian problems on ensuring information security of the Russian Federation involves: devising methodological framework for ensuring information security (including the determination of patterns of information environment as a system-creating factor of modern society), the establishment of information security theory as an interdisciplinary branch of science, the organization of its connection with other sciences; defining way and means to use information sphere in order to solve main social and political problems in Russia at the present stage; the development of legal enforcement of information security (including the legal regulation of the interests of the individual and society in the information sphere); the study of the importance and the role of information security problems in social processes of modern Russian society, in ensuring security of individual, mass and group consciousness, including an information and psychological security of the individual and society.

Conclusion. The study reveals one of the important scientific and practical tasks, such as the improvement of information security of municipal bodies. The findings of the study allow us to draw the appropriate conclusions.

Russian information area is aimed at playing the fundamental role in life of the Russian State. A prerequisite for this is to have sustainable information channels

which enable to know and to take into consideration public opinion in determining the priorities of social development. In order to avoid negative consequences of the transformation to the information society, it is necessary to draw great attention to the protection of interests of the State against new potential threats, in conjunction with organizational and legal methods of ensuring information security of municipal authorities.

The legislative framework of information security includes: unlimited-access information; limited-access information; injurious information; objects of intellectual property.

Information security in the bodies of state and municipal authority is rather specific. In order to prevent the leak of information, the authorities undertake a whole range of activities connected with regulatory acts containing state secret or confidential information.

The system of information security in municipal bodies is connected with the development of modern information technologies having advanced means to protect automated information systems and programmes for the implementation of electronic documents interaction.

Personal responsibility must be established for the use of data beyond the official duties or for private purposes. The effective method of control also implies combining technical means with administrative control measures. Limitation of functions performed with the documents which contain confidential data makes it possible to reduce the risk of information leaks to the external environment of administration. Internal processes streamlining, coordination and personnel management of administration departments of municipal district are the priority measures to enhance information protection of the local authority.

Information openness of a municipality is the groundwork of its image. In order to improve information openness of municipal bodies, it is necessary to elaborate a whole range of measures. Reception of citizens by deputies, mobile sittings of the committees in socially significant objects, deputy raids of control over implementation of regulations, both federal and local, should be organized.

The maximum accountability should be pursued in order to improve public confidence in municipalities, which, in particular, includes: establishing indicators of assessing and monitoring of public accountability of deputies; municipal practices including such elements as: the voters` right to information on the work of deputies; creating conditions for publicly available information on the activities of deputies according to the system of "a single window" where one might know the voting results, including the transcript of the speeches on different issues; radio programs, publications must meet the criteria of openness and transparency of their work and contain the elements of public report; compliance of election programs with deputies` activities; the development of the practices of citizen participation institute of public experts which assesses the performance of deputies; the development of practices of citizen`s participation in Duma`s sessions.

Municipal bodies should be guided by the principle of transparency, honesty and openness in their activities in order to avoid its being declarative in nature and to promote its sustainable development. Therefore, constant improvement of

providing transparency in municipal body activities is certainly the best way to raise the confidence of citizens in power structures and to modernize the bodies of state and municipal authorities.

Список литературы

1. *Аксенов С. Г.* Организационно-правовые основы обеспечения информационной безопасности органов государственной власти // Налоги. 2008. № 3 (2). С. 5–11.

2. *Арсентьев М. В.* Состояние информационной безопасности в России // Информационные ресурсы России. 2003. № 2. С. 19–21.

3. *Батурин Ю. М., Азишский А. М.* Компьютерная преступность и компьютерная безопасность. М. : Юрид. лит., 1991. 160 с.

4. *Вехов В. Б., Попова В. В., Ильюшин Д. А.* Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. Изд. 2-е, доп. и пр. М. : ЛексЭст, 2004. 160 с.

5. *Генна О. В.* Основные положения стеганографии // Защита информации конфиденциально. 2001. № 3. С. 20–25.

6. *Горшков Е. А., Саганова В. Н.* Обзор и анализ инструментальных средств обеспечения кадровой деятельности // Современные тенденции технических наук : материалы II Междунар. науч. конф. (г. Уфа, май 2013 г.). Уфа : Лето, 2013. С. 5–7.

7. *Донская Е. Н., Панко Ю. В.* Отдельные аспекты обеспечения информационной безопасности деятельности органов местного самоуправления // Молодой ученый. 2014. № 8. С. 453–457.

8. *Ковалев О. А., Беззубцев А. Н.* О лицензировании лицензирования и сертификации сертификации в области информационной безопасности. URL: http://www.cryptopro.ru/sites/default/-files/docs/licen.pdf (дата обращения: 02.02.2019).

9. *Круцких А., Крамаренко Г.* Дипломатия, информационно-коммуникационная революция // Международная жизнь. 2003. № 7. С. 102–113.

10. *Ляпунов Ю. И., Пушкин В. А.* Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / под ред. Н. А. Ветрова, Ж. И. Ляпунов. М. : [б. и.], 1998. С. 15–25.

11. *Панферова В. В.* Информационная политика в современной России // Социально-гуманитарные знания. 2005. № 5. С. 53- 68.

12. *Потрубач Н.Н.* Проблемы безопасности // Социально-гуманитарные знания. 1999. № 2. С. 264–273.

13. *Сиваков О. Г.* Актуальные проблемы информационной безопасности в научно-технической сфере // Информационные ресурсы России. 2003. № 4. С. 25–28.

14. Уголовное право Российской Федерации / отв. ред. Б. В. Здравомыслов. М.: Юристъ, 1996. 559 с.

15. Уголовное право / [В. Г. Беляев, А. И. Бойко, Н. И. Ветров [и др.]. М. : ПРИОР, 1999. 542 с.

16. *Черняк Л.* Новые задачи информационной безопасности // Открытые системы. СУБД. 2005. № 5/6. С. 16–18.

Информационная безопасность в муниципальных образованиях Забайкальского края

Т. Е. Бейдина, А. В. Новикова, А. Н. Кухарский

Забайкальский государственный университет, г. Чита, Российская Федерация

Аннотация. Информационная безопасность связана с увеличением как технических, так и информационных средств в политическом взаимодействии и пересмотром целей и задач государственных и муниципальных органов власти, органов обеспечения национальной, региональной и муниципальной безопасности. Переход в новое состояние по решению проблем функционирования информационной безопасности и новые задачи Российского государства и общества в современных условиях сопряжены с возникновением совершенно новых угроз как национальной безопасности в целом, так и ее основных составляющих – социально-политической и информационной безопасности. Данные угрозы необходимо преодолевать, в том числе путем интеграции новых информационных систем безопасности и модернизации информационных каналов связей. Актуализируется проблема обращения к депрессивному региону – Забайкальскому краю России. Данные обстоятельства указывают на необходимость переосмысления взглядов и разработки совершенно новых концептуальных подходов к вопросам информационной безопасности.

Ключевые слова: информационная безопасность, политический процесс, политическая коммуникация, коммуникационный процесс, национальная безопасность, управленческая коммуникация, электронная демократия.

Для цитирования: Бейдина Т. Е., Новикова А. В., Кухарский А. Н. Информационная безопасность в муниципальных образованиях Забайкальского края // Известия Иркутского государственного университета. Серия Политология. Религиоведение. 2019. Т. 30. С. 63–74. https://doi.org/10.26516/2073-3380.2019.30.63

References

1. Aksenov S.G. Organizacionno-pravovye osnovy obespecheniya informacionnoj bezopasnosti organov gosudarstvennoj vlasti [Organizational and legal bases of ensuring information security of public authorities]. *Taxes*, 2008, no. 3 (2), pp. 5-11. (in Russian)

2. Arsentiev M.V. Sostoyanie informacionnoj bezopasnosti v Rossii [The State of information security in Russia]. *Information resources of Russia,* 2003, no. 2, pp. 19-21. (in Russian)

3. Baturin Y.M., Azishskiy A.M. *Kompyuternaya prestupnost i komp'yuternaya bezopasnost* [Computer crime and computer security]. Moscow, Yurid. Literature Publ., 1991. 160 p. (in Russian)

4. Vekhov V.B., Popova V.V., Ilyushin D.A. *Takticheskie osobennosti rassledovaniya prestuplenij v sfere kompyuternoj informacii* [Tactical features of investigation of crimes in sphere of computer information: Scientific.-practice, manual]. 2-e ed. Moscow, Lexest Publ., 2004, 160 p. (in Russian)

5. Genne O.V. Osnovnye polozheniya steganografii [The main provisions of steganography]. *Information protection Confidential,* 2001, no. 3, pp. 20-25. (in Russian)

6. Gorshkov E.A., Saganova V.N. Obzor i analiz instrumentalnyh sredstv obespecheniya kadrovoj deyatelnosti [Review and analysis of tools for staffing]. *Modern trends in technical Sciences* (II): Proceedings of the Intern. highest level. scientific. conf. Ufa, may 2013. Ufa, Summer Publ., 2013, pp. 5-7. (in Russian)

7. Donskaya E.N., Panko Yu.V. Otdel'nye aspekty obespecheniya informacionnoj bezopasnosti deyatel'nosti organov mestnogo samoupravleniya [Separate aspects of ensuring information security of activity of local governments]. *Young scientist*, 2014, no. 8, pp. 453-457. (in Russian)

8. Kovalev O.A., Bezzubtsev A.N. *Licenzirovanii licenzirovaniya i sertifikacii sertifikacii v oblasti informacionnoj bezopasnosti* [About licensing licensing and certification of certification in the field of information security]. Available at: http://www.cryptopro.ru/sites/default/-files/docs/licen.pdf (data of access: 02.02.2019). (in Russian)

9. Krutskikh A., Kramarenko G. Diplomatiya, informacionno-kommunikacionnaya revolyuciya [Diplomacy, information and communication revolution]. *International life,* 2003, no. 7, pp. 102-113. (in Russian)

10. Lyapunov Y.I., Pushkin V.A. Prestupleniya v sfere kompyuternoj informacii [Crimes in sphere of the computer information]. *Criminal law. The special part*. Moscow, 1998, pp. 15-25 (in Russian)

11. Panferova V.V. Informacionnaya politika v sovremennoj Rossii [Information policy in modern Russia]. *Social and humanitarian knowledge*, 2005, no. 5, pp. 53-68. (in Russian)

12. Potrubach N.N. Problemy bezopasnosti [Security problems]. *Socially-humanitarian knowledge,* 1999, no. 2, pp. 264-273. (in Russian)

13. Sivakov O.G. Actual problems of information security in the scientific and technical sphere [Aktualnye problemy informacionnoj bezopasnosti v nauchno-tekhnicheskoj sfere]. *Information resources of Russia*, 2003, no. 4, pp. 25-28. (in Russian)

14. Zdravomyslov B.V. (ed.). *Ugolovnoe pravo Rossijskoj Federacii* [Criminal law of the Russian Federation]. Moscow, Lawyer Publ., 1996, 559 p. (in Russian)

15. Vetrov P.I., Belyaev V.G., Boyko A.I. *Ugolovnoe pravo* [Criminal law]. Moscow, Prior Publ., 1999, 542 p. (in Russian)

16. Chernyak L. Novye zadachi informacionnoj bezopasnosti [New tasks of information security]. *Open systems. DBMS*, 2005, no. 5/6, pp.16-18. (in Russian)

Бейдина Татьяна Евгеньевна
доктор политических наук, профессор, заведующая, кафедра государственного, муниципального управления и политики, Забайкальский государственный университет
Российская Федерация, 672039, г. Чита, ул. Александро-Заводская, 30
тел.: 8(3022)417336
e-mail: beydina@inbox.ru

Beydina Tatiana Evgenievna
Doctor of Sciences (Political Science), Professor, Head, Department of State and Municipal Administration and Politics TransBaikal State University
30, Aleksandro-Zavodskaya st., Chita, 672039, Russian Federation
tel.: 8(3022)417336
e-mail: beydina@inbox.ru

Новикова Анна Владимировна
кандидат политических наук, доцент, кафедра государственного, муниципального управления и политики
Забайкальский государственный университет
Российская Федерация, 672039, г. Чита, ул. Александро-Заводская, 30
тел.: 8(3022)417336
e-mail: anna_novikova2010@mail.ru

Novikova Anna Vladimirovna
Candidate of Sciences (Political Science), Associate Professor, Department of State and Municipal Administration and Politics Transbaikal State University
30, Aleksandro-Zavodskaya st., Chita, 672039, Russian Federation
tel.: 8(3022)417336
e-mail: anna_novikova2010@mail.ru

Кухарский Артем Николаевич
аспирант, кафедра государственного, муниципального управления и политики
Забайкальский государственный университет
Российская Федерация, 672039, г. Чита, ул. Александро-Заводская, 30
тел.: 8(3022)417336
e-mail: kukharskijjartjom@yandex.ru

Kukharsky Artem Nikolaevich
Postgraduate, Department of State and Municipal Administration and Politics Transbaikal State University
30, Aleksandro-Zavodskaya st., Chita, 672039, Russian Federation
tel.: 8(3022)417336
e-mail: kukharskijjartjom@yandex.ru

Дата поступления: 23.08.2019
Received: August, 02, 2019