Doctrine of Information Security of the Russian Federation

APPROVED
by Decree of the President
of the Russian Federation
No. 646 of December 5, 2016

I. General Provisions

1. This Doctrine constitutes a system of official views on ensuring the national security of the Russian Federation in the information sphere.

The Doctrine defines the information sphere as a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet (hereinafter referred to as the "Internet"), communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere.

2. The Doctrine uses the following basic notions:

a) the national interests of the Russian Federation in the information sphere (hereinafter referred to as the "national interests in the information sphere") are the objectively meaningful needs of the individual, society and the State in ensuring their safety and security and sustainable development in the information sphere;

b) the threat to the information security of the Russian Federation (hereinafter referred to as the "information threat") is a combination of actions and factors creating a risk of damaging the national interests in the information sphere;

c) the information security of the Russian Federation (hereinafter referred to as the "information security") is the state of protection of the individual, society and the State against internal and external information threats, allowing to ensure the constitutional human and civil rights and freedoms, the decent quality and standard of living for citizens, the sovereignty, the territorial integrity and sustainable socio-economic development of the Russian Federation, as well as defence and security of the State;

d) the provision of information security is the implementation of mutually supportive measures (legal, organizational, investigative, intelligence, counter-intelligence, scientific and technological, information and analytical, personnel-related, economic and others) to predict, detect, suppress, prevent, and respond to information threats and mitigate their impact;

e) information security forces are government bodies, as well as units and officials of government bodies, local authorities and organizations tasked to address information security issues in accordance with the legislation of the Russian Federation;

f) information security means are legal, organizational, technical and other means used by information security forces;

g) the information security system is a combination of information security forces engaged in coordinated and planned activities, and information security means they use;

h) the information infrastructure of the Russian Federation (hereinafter referred to as the "information infrastructure") is a combination of informatization objects, information systems, Internet websites and communication networks located in the territory of the Russian Federation, as well as in the territories under the jurisdiction of the Russian Federation or used under international treaties signed by the Russian Federation.

3. Based on the analysis of major information threats and assessment of the state of information security, the Doctrine defines the strategic objectives and key areas of information security taking into account the strategic national priorities of the Russian Federation.

4. The Constitution of the Russian Federation, universally recognized principles and norms of international law, international treaties signed by the Russian Federation, federal constitutional laws, federal laws, as well as normative legal acts of the President of the Russian Federation and the Government of the Russian Federation form the legal framework of the Doctrine.

5. The Doctrine is a strategic planning document on ensuring the national security of the Russian Federation, which builds upon the provisions of the National Security Strategy of the Russian Federation approved by the Decree of the President of the Russian Federation No. 683 of December 31, 2015, and other strategic planning documents in this area.

6. The Doctrine provides the basis for the development of the State policy and public relations in the sphere of information security, as well as for the elaboration of measures to improve the information security system.

II. National Interests in the Information Sphere

7. Information technologies have become global and transboundary in their nature and are now an integral part of all areas of activity of the individual, society and the State. Effective use of these technologies will promote the national economic growth and the development of information societies.

The information sphere has a crucial role to play in the implementation of the strategic national priorities of the Russian Federation.

8. National interests in the information sphere include:

a) ensuring and protecting constitutional human and civil rights and freedoms with regard to the receipt and use of information; privacy in the use of information technologies, providing information support to democratic institutions and mechanisms of interaction between the State and civil society; as well as applying information technologies for the preservation of cultural, historical, spiritual and moral values of the multi-ethnic people of the Russian Federation;

b) maintaining the sustainable and smooth operation of the information infrastructure, primarily of the critical information infrastructure of the Russian Federation (hereinafter referred to as the "critical information infrastructure"), and the integrated telecommunications network of the Russian Federation, in peacetime, in the event of a direct threat of aggression, and in wartime;

c) developing the sector of information technologies and electronics in the Russian Federation and improving the performance of production, research and scientific and technological community to develop, produce and operate information security means and provide information security services;

d) providing the Russian and international community with reliable information on the State policy of the Russian Federation and its official position on socially significant events in Russia and in the world, and applying information technologies to ensure the national security of the Russian Federation in the sphere of culture;

e) facilitating the development of an international information security system aimed at countering threats of the use of information technologies to compromise the strategic stability, at strengthening equal strategic partnership in the sphere of information security, as well as protecting the information sovereignty of the Russian Federation.

9. Realization of national interests in the information sphere aims at shaping a safe environment for the circulation of reliable information, and an information infrastructure capable of resisting different kinds of impacts in order to guarantee constitutional human and civil rights and freedoms, the sustainable socio-economic development, as well as the national security of the Russian Federation.

III. Major Information Threats and the State of Information Security

10. While a wider use of information technologies contributes to economic development and better functioning of social and State institutions, it also gives rise to new information threats.

The possibilities of transboundary information circulation are increasingly used for geopolitical goals, goals of a military-political nature contravening international law or for terrorist, extremist, criminal and other unlawful ends detrimental for international security and strategic stability.

Moreover, the practice of adopting information technologies without due consideration of their impact on information security significantly increases the probability of information threats.

11. One of the key negative factors affecting the state of information security is the fact that a number of foreign countries are building up their information technology capacities to influence the information infrastructure in pursuing military purposes.

At the same time, the organizations engaged in technical intelligence with regard to Russian government bodies, research organizations and enterprises of defence-industrial complex are stepping up their activities.

12. Intelligence services of certain States are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end.

There is a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation.

Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties.

There is a growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values.

13. Various terrorist and extremist organizations widely use information tools to influence individual, group and public consciousness in order to fester interethnic and social tensions, incite ethnic or religious hatred or hostility, spread extremist ideology, as well as recruit new supporters of terrorist activities. These organizations actively develop destructive tools to impact critical information infrastructure objects for illegal purposes.

14. There is a rise in computer crimes, primarily in credit and financial sphere. The number of crimes related to violation of constitutional, human and civil rights and freedoms, including with respect to privacy, personal and family life, in the processing of personal data with the use of information technologies, is also increasing. The methods, means and tools used to commit such crimes get more and more sophisticated.

15. Information security in the sphere of national defence is characterised by the growing use by certain States and organizations of information technologies for military and political purposes, including for actions inconsistent with international law and seek to undermine the sovereignty, political and social stability and territorial integrity of the Russian Federation and its allies, and pose a threat to international peace, global and regional security.

16. Information security in the sphere of State and social security is characterised by a continued increase in the complexity, scope, and coordination of computer attacks on objects of critical information infrastructure, enhanced intelligence activities of foreign States against the Russian Federation, as well as growing risk that information technologies will be used to infringe on the sovereignty, territorial integrity, or political and social stability of the Russian Federation.

17. Information security in the economic sphere is characterised by a lack of competitive information technologies and the inadequate use of information technologies in the production of goods and services. The level of dependence of the domestic industry on foreign information technologies, such as electronic components, software, computers and telecommunications equipment remains high, which makes the socioeconomic development of the Russian Federation dependent on the geopolitical interests of foreign countries.

18. Information security in the sphere of science, technology and education is characterised by a need for greater efficiency in scientific research designed to create advanced information technologies, the limited use of national technologies and lack of staff in the information security sphere, as well as by the low level of public awareness of personal information security matters. At the same time, there is often no comprehensive framework for ensuring safety of information infrastructure, including its integrity, availability and stable functioning, using domestic information technology and products.

19. Information security in the sphere of strategic stability and equitable strategic partnership is characterised by the desire of individual States to use their technological superiority to dominate the information space.

Given the current global distribution of resources required to ensure safe and steady functioning of the Internet, it is not possible to manage them jointly in a fair and trust-based manner.

The absence of international legal norms regulating inter-State relations in the information space, as well as mechanisms and procedures for their application that would take into account the specifics of information technologies makes it difficult to create an international information security system designed to achieve strategic stability and equitable strategic partnership.

IV. Strategic Objectives and Key Areas of Ensuring Information Security

20. A strategic objective of ensuring information security in the field of national defence is to protect the vital interests of the individual, society and the State from both internal and external threats related to the use of information technologies for military and political purposes that run counter to international law, including for the purposes of taking hostile actions and acts of aggression that undermine the sovereignty and territorial integrity of States and pose a threat to international peace, security and strategic stability.

21. The military policy of the Russian Federation identifies the following key areas of ensuring information security in the field of national defence:

a) ensuring strategic deterrence and preventing military conflicts that may be brought about by the use of information technologies;

b) upgrading the information security system of the Armed Forces of the Russian Federation, other troops, military formations and bodies, including forces and means of information confrontation;

c) forecasting, identifying and assessing information threats, including threats to the Armed Forces of the Russian Federation in information sphere;

d) promoting the interests of the Russian Federation's allies in information sphere;

e) countervailing information and psychological actions, including those aimed at undermining the historical foundations and patriotic traditions related to defending the homeland.

22. The strategic objectives of efforts to ensure information security related to the State and public security are to protect the sovereignty, maintain political and social stability, and territorial integrity of the Russian Federation, uphold fundamental human and civil rights and freedoms, as well as to protect the critical information infrastructure.

23. The main thrusts of the information security related to State and public security are the following:

a) countering the use of information technologies to promote extremist ideology, spread xenophobia and ideas of national exceptionalism for the purposes of undermining the sovereignty, political and social stability, forcible changing the constitutional order and violating the territorial integrity of the Russian Federation;

b) suppressing the activity detrimental to the national security of the Russian Federation, carried out by special services and organizations of foreign States as well as by individuals using technical means and information technologies;

c) enhancing the protection of the critical information infrastructure and reliability of it’s functioning, developing mechanisms of identification and prevention of information security threats and elimination of their effects, as well as enhancing the protection of citizens and territories from the effects of emergencies caused by information and technical impacts on the objects of critical information infrastructure;

d) enhancing the safe operation of information infrastructure objects, including with a view to ensuring stable interaction between government bodies, preventing foreign control over these objects, and ensuring the integrity, smooth operation and safety of the unified telecommunications network of the Russian Federation, as well as ensuring the security of information transferred through this network and processed within information systems in the territory of the Russian Federation;

e) enhancing the secure and safe operation of weapons, military and special equipment and automated control systems;

f) enhancing the effectiveness of prevention of offences involving the use of information technologies, and countering such offences;

g) protecting information constituting the State secret, and other restricted access and dissemination information, including through improving the security of the relevant information technologies;

h) improving the methods and techniques of the manufacturing and safe use of goods and provision of services based on domestic information technologies complying with information security requirements;

i) improving information support activities to implement the State policy of the Russian Federation;

j) neutralizing the information impact intended to erode Russia's traditional moral and spiritual values.

24. The strategic objectives of information security in the field of economy are to minimize the impact of negative factors caused by the insufficient development of the Russian sector of information technologies and electronics, to develop and produce competitive information security means, as well as to increase the volume and improve the quality of information security services.

25. The main thrusts of ensuring information security in the field of economy are the following:

a) promoting the innovative development of the information technologies and electronics sector and increasing the share of its products in the national gross domestic product and exports;

b) eliminating the dependence of domestic industries on foreign information technologies and information security means by creating, developing and widely implementing Russian solutions, as well as producing goods and providing services based on such solutions;

c) improving the competitiveness of Russian companies engaged in the information technologies and electronics sector that develop, produce and operate information security means and provide information security services, including by creating favourable operating environment in the territory of the Russian Federation;

d) developing a competitive domestic electronic component base and technologies for producing electronic components, meeting the needs of the domestic market in such products and promoting them in the global market.

26. A strategic objective of ensuring information security in science, technology and education is to support the innovative and accelerated development of the information security system, as well as the information technologies and electronics sector.

27. The main thrusts of ensuring information security in science, technology and education are the following:

a) making Russian information technologies competitive and developing the country's information security scientific and technological capability;

b) developing and implementing information technologies inherently resilient to various types of impact;

c) conducting research and development with a view to producing prospective information technologies and information security means;

d) developing human resources in the field of information security and the use of information technologies;

e) protecting citizens from information threats, including by promoting the culture of personal information security.

28. A strategic objective of information security in the field of strategic stability and equal strategic partnership is to create a sustainable system of conflict-free inter-State relations in the information space.

29. The main thrusts of ensuring information security in the field of strategic stability and equal strategic partnership are the following:

a) protecting the sovereignty of the Russian Federation in information space through nationally-owned and independent policy to pursue its national interests in information sphere;

b) taking part in establishing an international information security system capable of effectively countering the use of information technologies for military and political purposes that are contrary to international law, or for terrorist, extremist, criminal or other illegal purposes;

c) creating international legal mechanisms taking into account the specific nature of information technologies and intended to prevent and settle conflicts between States in information space;

d) promoting in international organizations the position of the Russian Federation advocating equitable and mutually beneficial cooperation of all interested parties in information sphere;

e) developing a national system of the Russian Internet segment management.

V. Institutional Framework of Information Security

30. The information security system is part of the broader national security system of the Russian Federation.

Information security is ensured through the combination of legislative, law enforcement, judicial, oversight and other activities of government bodies working in cooperation with local governments, organizations and citizens.

31. The information security system is functioning on the basis of distribution of competencies among the legislative, executive and judicial bodies in this sphere, with due regard for the competence of federal authorities, the authorities of the constituent entities of the Russian Federation and local governments determined by security laws of the Russian Federation.

32. The structure of the information security system is determined by the President of the Russian Federation.

33. The institutional framework of the information security system is made up of: the Council of the Federation of the Federal Assembly of the Russian Federation, the State Duma of the Federal Assembly of the Russian Federation, the Government of the Russian Federation, the Security Council of the Russian Federation, federal executive bodies, the Central Bank of the Russian Federation, the Military-Industrial Commission of the Russian Federation, inter-agency bodies established by the President and Government of the Russian Federation, executive bodies of the constituent entities of the Russian Federation, local governments and judicial bodies involved in information security activities in accordance with the laws of the Russian Federation.

The information security system includes the following actors: owners of critical information objects and organizations operating such objects; mass media and mass communications; monetary, foreign currency, banking and other financial institutions; telecommunication operators; information system operators; organizations that create and operate information and communications systems; organizations that develop, produce and operate information security means; organizations that provide information security services; organizations that provide education services in this sphere; public associations and other organizations and individuals involved in information security under the laws of the Russian Federation.

34. Information security activities of government bodies is based on the following principles:

a) the legality of public relations in information sphere and the legal equality of all participants of such relations arising from the constitutional right of citizens freely to seek, receive, transmit, produce and disseminate information in any legal manner;

b) constructive interaction between government bodies, organizations and citizens in dealing with information security tasks;

c) maintaining a balance between citizens' demand for the free exchange of information and restrictions related to national security, including in information sphere;

d) the adequacy of information security forces and means determined, inter alia, through constant monitoring of information threats;

e) compliance with the universally recognized principles and norms of international law, international treaties to which the Russian Federation is a party and laws of the Russian Federation.

35. The government bodies pursue the following objectives in the sphere of information security:

a) protecting the rights and legitimate interests of citizens and organizations in information sphere;

b) assessing the information security state, forecasting and identifying information threats, determining priority areas for their prevention and remedying their effects;

c) planning, implementing and assessing the effectiveness of information security measures;

d) organizing the activities and coordinating the interaction of information security forces and improving their legal, organizational, operative investigation, intelligence, counter-intelligence, scientific and technical, information and analytical, staffing and economic support;

e) developing and implementing measures of State support to organizations that develop, produce and operate information security means, organizations that provide information security services, and organizations that provide education services in this sphere.

36. In their activities to develop and improve the information security system, the government bodies pursue the following objectives:

a) strengthening the vertical management system and centralizing information security forces at the federal, inter-regional, regional and municipal levels, as well as at the level of informatization objects, and operators of information systems and communication networks;

b) improving the forms and methods of interaction between information security forces to enhance their preparedness to countering information threats, including through regular drills (exercises);

c) improving information, analytical and scientific and technical aspects of the operation of the information security system;

d) enhancing the efficiency of interaction between government agencies, local governments, organizations and citizens to perform information security tasks.

37. The Doctrine shall be implemented in accordance with sectoral strategic planning documents of the Russian Federation. To keep these documents updated, the Security Council of the Russian Federation shall compile a list of medium-term priority areas of information security taking into account the provisions of the strategic outlook for the Russian Federation.

38. The findings of monitoring the implementation of this Doctrine shall be included in the annual report on national security and measures to enhance it presented by the Secretary of the Security Council of the Russian Federation to the President of the Russian Federation.

Доктрина информационной безопасности Российской Федерации
Конвенция об обеспечении международной информационной безопасности (концепция)
Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года
Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации
Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Doctrine of Information Security of the Russian Federation

- Главная страница