INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION

Approved by President of the Russian Federation Vladimir Putin on September 9, 2000

29-12-2008

The Information Security Doctrine of the Russian Federation represents a totality of official views on the goals, objectives, principles and basic guidelines for ensuring information security in the Russian Federation.

The present Doctrine serves as the basis for:

- shaping government policy on information security in the Russian Federation;

- preparing suggestions to improve the legal, procedural, scientific-technical and organizational framework for ensuring information security in the Russian Federation;

- devising targeted national information security programs.

The present Doctrine expounds the National Security Concept of the Russian Federation as applied to the information sphere.

I. INFORMATION SECURITY OF THE RUSSIAN FEDERATION

1. The national interests of the Russian Federation in the information sphere and how they are to be secured

The present stage in societal development is characterized by an increasing role of the information sphere, which represents an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions. The information sphere as a system-forming factor of societal life actively influences the state of the political, economic, defense, and other components of Russian Federation security. The national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase.

By the information security of the Russian Federation is meant the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state.

The interests of the individual in the information sphere consist of the exercise of the constitutional rights of man and the citizen to information access, to use of information in the interest of carrying on activities not prohibited by law and of physical, spiritual and intellectual development, as well as of the protection of information that ensures personal security.

The interests of society in the information sphere consist of securing the interests of the individual in this sphere, reinforcing democracy, creating a rule-of-law social state, achieving and maintaining public harmony and of the spiritual renewal of Russia.

The state's interests in the information sphere consist of creating conditions for harmonious Russian information infrastructure development and for the exercise of the constitutional rights and freedoms of man and the citizen with respect to receiving and using information to ensure the inviolability of the constitutional system, the sovereignty and territorial integrity of Russia, and political, economic and social stability; the interests of the state also consist in the unconditional maintenance of law and order and in the promotion of equal and mutually advantageous international cooperation.

Based on the national interests of the Russian Federation in the information sphere, the state forms its strategic and current domestic and foreign policy objectives for ensuring information security.

Four ingredients of the national interests of the Russian Federation stand out as most salient in the information sphere.

The first ingredient of Russia's national interests in the information sphere comprises observance of the constitutional rights and freedoms of man and the citizen to receive and use information, the assurance of a spiritual renewal of Russia, and the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country.

Achieving this requires:

- raising information infrastructure use efficiency for the sake of social development, the consolidation of Russian society, and the spiritual rebirth of the multinational people of the Russian Federation;

- streamlining the system of formation, preservation and rational utilization of information resources that form the basis of the scientific, technical and spiritual potential of the Russian Federation;

- securing the constitutional rights and freedoms of man and the citizen freely to seek, receive, transmit, produce and disseminate information by any legal means and to get reliable information about the state of the environment;

- securing the constitutional rights and freedoms 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;

- reinforcing the mechanisms of legal governance of relations in the field of intellectual property protection, and creating conditions for observance of the federally prescribed restrictions on access to confidential information;

- guaranteeing the freedom of mass information and the prohibition of censorship;

- not allowing for propaganda or campaigning that serves to foment social, racial, national or religious hatred and strife;

- securing a ban on the collection, storage, use and dissemination of information about the private life of persons without their consent and of any other information to which access is restricted by federal legislation.

The second ingredient of the national interests of the Russian Federation in the information sphere comprises information support for the state policy of the Russian Federation that involves conveying to the Russian and international public trustworthy information about the state policy of the Russian Federation and about its official position on socially significant events in Russian and international life, with the provision of access for citizens to open government information resources.

Achieving this requires:

- bolstering the state mass media, expanding their capabilities to promptly convey reliable information to Russian and foreign citizens;

- intensifying the formation of open government information resources and raising the efficiency in their practical use.

The third ingredient of the national interests of the Russian Federation in the information sphere comprises promoting modern information technologies, boosting the national information industry (the industries of informatization, telecommunication, 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. Problems in developing high technologies, retooling industry, and multiplying achievements in national science and technology can be solved only on this basis under present-day conditions. Russia must occupy a worthy position among world microelectronic and computer industry leaders.

Achieving this requires:

- developing and improving 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;

- providing government support of Russian fundamental and applied research, and developments in the areas of informatization, telecommunication and communication.

The fourth ingredient of the national interests of the Russian Federation in the information sphere comprises protecting information resources against unsanctioned access, and securing the information and telecommunication systems whether already deployed or being set up on the territory of Russia.

For these purposes it is necessary to:

- enhance the security of information systems including communication networks, primarily 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 financial, and banking spheres, the sphere of economic activity as well as the security of systems and means for informatizing weapons and military equipment, security of troop and arms control systems, and the security of management systems for environmentally hazardous and economically important enterprises;

- intensify development of the domestic production of information protection hardware and software, along with the methods to control their efficiency;

- secure data that constitute state secrets;

- expand international cooperation by the Russian Federation with respect to the development and secure utilization of information resources and counteraction against the threat of rivalry in the information sphere.

2. Types of threats to the information security of the Russian Federation

According to their general directionality, threats to the information security of the Russian Federation are subdivided into the following types:

- threats to the constitutional rights and freedoms of man and the citizen in the area of spiritual life and information activities, to individual, group and public consciousness and to Russia's spiritual revival;

- threats to information support to Russian Federation state policy;

- threats to Russian information industry (including informatization, telecommunication, and communication facilities) development, to the satisfaction of domestic market requirements with its products and their entry into the world market, and to the accumulation, storage reliability, and effective utilization of national information resources;

- threats to the security of information and telecommunication systems and facilities whether already deployed or being set up on the territory of Russia.

The threats to the constitutional rights and freedoms of man and the citizen in the areas of spiritual life and information activities, to individual, group and public consciousness and to Russia's spiritual revival may be as follows:

- adoption by federal bodies of state authority or by bodies of state authority in constituent entities of the Russian Federation 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 in the Russian Federation with the use of telecommunication systems or otherwise;

- 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;

- irrational, excessive restrictions placed on access to socially necessary information;

- illegal use of special means of influence on individual, group and public consciousness;

- noncompliance by federal bodies of state authority, by bodies of state authority in constituent entities of the Russian Federation, by bodies of local self-government 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 the federal bodies of state authority, the bodies of state authority of the constituent entities of the Russian Federation or bodies of local self-government, to open archival materials and to other open socially significant information;

- disorganization or destruction of a system of accumulation and preservation of cultural properties, including archives;

- violation of the constitutional rights and freedoms of man and the citizen in the field of mass information;

- ousting of Russian news agencies and media from the national information market, and an increase in dependence of the spiritual, economic and political areas of public life in Russia on foreign information entities;

- depreciation of spiritual values, the propaganda of specimens of mass culture based on the cult of violence or on spiritual and moral values contrary to the values adopted in Russian society;

- a decrease in the spiritual, moral and creative potential of the Russian population that would substantially complicate training manpower resources for adoption and use of newest (including 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 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 threats to the national information industry (the industries of informatization, telecommunication, and communication facilities in particular), to the satisfaction of domestic market requirements with its products and their entry into the world market, as well as to the accumulation, storage reliability, and effective utilization of national information resources may be as follows:

- opposition to access by the Russian Federation to newest information technologies, to the mutually advantageous and equal participation of Russian producers in the world division of labor in the industry of information services, means of informatization, telecommunication

and communication and information products, as well as the creation of conditions for increasing Russia's dependence in the field of modern information technologies;

- purchases of imported means of informatization, telecommunication and communication by government bodies when domestic analogues not inferior to the foreign samples in their characteristics are available;

- the ousting from the domestic market of Russian producers of means of informatization, telecommunication and communication;

- an increase in the outflow of specialists and intellectual property rights holders going abroad.

The threats to the security of the information and telecommunication systems and facilities whether already deployed or being set up on the territory of Russia may be as follows:

- 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 technology systems, including information security systems;

- destruction, damage, disturbance of, or electronic attack against information processing, telecommunication and communication systems and means;

- 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 or into office premises of government bodies, enterprises, institutions or organizations under whatever form of ownership;

- destruction, damage, disturbance or theft of machine processable data carriers;

- interception of information in data transmission networks or on communication lines, deciphering of this information and foisting of false information;

- use of uncertified domestic and foreign information technologies, information protection means and informatization, telecommunication and communication facilities in setting up and developing the Russian information infrastructure;

- unsanctioned access to information contained in databanks or databases;

- breach of the lawful restrictions on information dissemination.

3. Sources of threats to the information security of the Russian Federation

The sources of threats to the information security of the Russian Federation are subdivided into external and internal.

To the external sources belong:

- activities of foreign political, economic, military, intelligence and information entities, directed against the interests of the Russian Federation in the information sphere;

- the striving of a number of countries toward dominance and the infringement of Russia's interests in the world information space and to oust it from external and domestic information markets;

- toughened international competition for information technologies and resources;

- activities of international terrorist organizations;

- an increase in the technological edge of leading world powers and the buildup of their ability to hinder the creation of competitive Russian information technologies;

- space, air, sea and land technical and other means (types) of reconnaissance activities on the part of foreign states;

- development by a number of states of information war concepts that provide for creating means for dangerous attack on the information spheres of other countries of the world, disturbing the normal functioning of their information and telecommunication systems, breaching the security of their information resources and gaining unsanctioned access to them.

To the internal sources belong:

- a critical state of national branches of industry;

- an unfavorable criminogenic situation accompanied by tendencies for coalescence between state and criminal structures in the information sphere, for criminal structures to gain access to confidential information, for greater influence of organized crime on the life of society, for a decrease in the level of protection of the lawful interests of citizens, society and the state in the information sphere;

- insufficient coordination among the federal bodies of state authority and the bodies of state authority of the constituent entities of the Russian Federation in shaping and carrying out a unified state policy in the realm of national information security;

- an insufficient degree of development of the legal and regulatory base governing relations in the information sphere, and inadequate law enforcement practices;

- the immaturity of civil society institutions, and insufficient state control over the development of the Russian information market;

- insufficient financing for measures aimed at ensuring the information security of the Russian Federation;

- insufficient economic power of the state;

- the decline in efficiency of the system of education and upbringing, insufficient numbers of qualified personnel in the realm of information security;

- insufficient vigor of federal bodies of state authority or bodies of state authority of constituent entities of the Russian Federation in informing society about their activities, in explaining their decisions, in forming open government resources and in developing a system of access to them for citizens;

- Russia's lag behind the world's leading countries in level of informatization of federal bodies of state authority, the bodies of state authority of the constituent entities of the Russian Federation and bodies of local-self government, the financial and credit sphere, industry, agriculture, education, public health, and consumer services.

4. The state of information security of the Russian Federation and the main challenges in its assurance

In recent years the Russian Federation has carried out a set of measures to improve its information security.

Shaping a legal framework for information security has begun. The State Secrets Law and the Fundamental National Archives and Records Legislation of the Russian Federation, along with the Federal Laws on Information, Informatization and Information Protection and on Participation in International Information Exchange and a number of other laws, have been adopted, and work has been launched to create the relevant implementation mechanisms and to craft laws governing public relations in the information sphere.

Information security measures have been carried out in the federal bodies of state authority, in the bodies of state authority of the constituent entities of the Russian Federation and in enterprises, institutions and organizations under whatever form of ownership. Work has been launched to set up a protected special-purpose information technology system in the interests of the bodies of state authority.

The successful tackling of information security issues in the Russian Federation is aided by the national system of information protection, the system for protecting state secrets, the systems for licensing activities in the field of the protection of state secrets and the systems for certifying information protection tools.

Yet analysis of the state of information security in the Russian Federation shows that its level is not fully consistent with the requirements of society and the state.

The current political and socioeconomic development conditions in the country give rise to sharp contradictions between the requirements of society in a wider free exchange of

information and the necessity of retaining individual regulated limitations on its dissemination.

The contradictory nature and immaturity of the legal governance of social relations in the information sphere lead to serious negative consequences. Thus, the insufficiency of a legal and regulatory framework for relations in the field of realization of the possibilities for constitutional restrictions on mass media freedom in the interests of protecting the foundations of the constitutional system and the morality, health, rights and lawful interests of citizens, ensuring national defense capability and state security considerably impede the maintenance of a balance of interests among the individual, society and the state in the information sphere. Imperfect legal and normative governance of relations in the field of mass information hampers the establishment of competitive Russian news agencies and media within the territory of the Russian Federation.

The precariousness of citizens' rights to information access, and information manipulation evoke a negative reaction among people, which in a number of cases leads to a destabilization of the social and political situation in society.

The constitutionally enshrined rights of citizens to the inviolability of private life, to personal and family privacy and the privacy of correspondence essentially do not have a sufficient legal, organizational and technical backing. Unsatisfactorily organized is the protection of personal data referring to natural persons that are collected by federal bodies of state authority, those of the constituent entities of the Russian Federation and bodies of local self-government.

The lack of efficiency in pursuing a state policy in efforts to create the Russian information space, develop the mass information system, organize international information exchange and integrate the Russian information space into the world information space engenders conditions for ousting Russian news agencies and media from the national information market and for distorting the structure of international information exchange.

Insufficient is government support to the activities of Russian news agencies in promoting their products to the foreign information market.

The situation with ensuring the security of data that constitute state secrets is deteriorating.

Serious damage has been inflicted upon the cadre potential of scientific and production collectives operating in the development and manufacture of informatization, telecommunication and communication means owing to their most qualified specialists' departure therefrom.

The lag of national information technologies forces the federal bodies of state authority, bodies of state authority of the constituent entities of the Russian Federation and bodies of local self-government to purchase import equipment when establishing information systems and to enlist foreign firms, because of which the likelihood of unsanctioned access to the information being processed increases and Russia's dependence on foreign computer and telecommunication hardware and software manufacturers grows.

In the wake of an intensive introduction of foreign information technologies in the areas of activity of the individual, society and the state, and following the wide use of open information technology systems and the integration of national information systems and international information systems the threats of the use of the "information weapon" against

the Russian information infrastructure have increased. Work on an adequate and comprehensive response to these threats is being conducted with insufficient coordination and poor budget financing. Not enough attention is being given to the development of space reconnaissance and electronic warfare systems.

The resultant state of affairs in the area of information security in the Russian Federation requires an immediate solution of such **tasks** as:

- developing basic guidelines for state policy in the area of information security in the Russian Federation as well as measures and mechanisms connected with the implementation of this policy;

- developing and improving the national information security system that realizes a unified state policy in this field, including upgrading the forms, methods and techniques of identification, assessment and prediction of information security threats, along with the system to counteract these threats;

- developing federal purpose-oriented programs of ensuring the information security of the Russian Federation;

- developing criteria and methods for assessing the effectiveness of, and certifying national information security systems and means;

- streamlining the legal and regulatory base for national information security, including the mechanisms for realizing citizens' rights to obtain and access information, and the forms and methods for carrying out the legal norms concerning state-media interaction;

- the establishment of the responsibility of officials of the federal bodies of state authority, bodies of state authority of the constituent entities, bodies of local self-government and of legal entities and citizens for the observance of information security requirements;

- coordinating the activities of the federal bodies of state authority, the bodies of state authority of the constituent entities, enterprises, institutions and organizations under whatever form of ownership in the field of ensuring the information security of the Russian Federation;

- developing the theoretical and practical foundations of national information security assurance with regard for the current geopolitical situation, Russia's political and socioeconomic development conditions and the reality of the use of the "information weapon";

- crafting and setting up mechanisms to shape and implement the state information policy of Russia;

- developing methods for raising the effectiveness of state participation in shaping the information policy of state television and radio broadcasting organizations and other state-run mass media;

- securing the technological independence of the Russian Federation in the major areas of informatization, telecommunications and communication determining its security, and

primarily in the field of developing specialized computer hardware for weapon and military equipment specimens;

- devising contemporary methods and tools for protecting information and securing information technologies, primarily those used in troop and weapons control systems and in management systems for environmentally hazardous and economically important enterprises;

- developing and improving the state system of information protection and the system for the protection of state secrets;

- creating and developing a contemporary protected technological base of government in peacetime, in emergencies and in wartime;

- expanding cooperation with international and foreign agencies and organizations in dealing with scientific-technical and legal issues in securing information that is transmitted with the aid of international telecommunication and communication systems;

- providing conditions for active development of the Russian information infrastructure and for the participation of Russia in the processes of the creation and use of global information networks and systems;

- creating a unified system of personnel training in the area of information security and information technologies.

II. METHODS FOR ENSURING THE INFORMATION SECURITY OF THE RUSSIAN FEDERATION

5. General methods for ensuring the information security of the Russian Federation

The general methods for ensuring the information security of the Russian Federation are subdivided into legal, organizational-technical and economic.

The legal methods of ensuring the information security of the Russian Federation include the development of normative legal acts governing relations in the information sphere and normative procedural documents related to national information security assurance. The most important areas of this activity are as follows:

- introducing amendments and addenda to the Russian Federation legislation governing relations in the realm of information security with a view to the establishment and streamlining of the system for ensuring the information security of the Russian Federation, removal of inner contradictions in the federal legislation, contradictions relating to the international agreements to which the Russian Federation has acceded, and contradictions between federal legislative acts and legislative acts of constituent entities of the Russian Federation, as well as for the purpose of concretizing the legal norms establishing responsibility for law violations in the field of ensuring the information security of the Russian Federation;

- the legislative division of power in the field of national information security between the federal bodies of state authority and those of the constituent entities of the Russian

Federation and the determination of the goals, objectives and mechanisms of participation by public associations, organizations and citizens in this activity;

- crafting and adopting normative legal acts of the Russian Federation to establish legal and natural persons' responsibility for unsanctioned access to, and the illegal copying, distortion or unlawful use of information, the deliberate circulation of untrue information, the illegal disclosure of confidential information and the use of business or trade secret information for criminal or ulterior purposes;

- making more precise the status of foreign news agencies, media and journalists as well as of investors when attracting foreign investment for the development of Russia's information infrastructure;

- the legislative entrenchment of development priority for national communication networks and domestic production of communications satellites;

- determination of the status of organizations providing the services of global information technology networks within the territory of the Russian Federation, and the legal regulation of the activities of these organizations;

- creation of a legal base for the formation of regional information security structures in the Russian Federation.

The organizational-technical methods for ensuring the information security of the Russian Federation are as follows:

- establishing and improving the system for ensuring the information security of the Russian Federation;

- enhancing law enforcement activities of federal executive bodies and those of the constituent entities of the Russian Federation, including the prevention and suppression of law violations in the information sphere, as well as identifying, proving guilty and bringing to justice those responsible for crimes or other violations committed in this sphere;

- development, use and perfecting of information protection resources and tools for monitoring the effectiveness thereof, the development of protected telecommunication systems and enhancement of the reliability of special software;

- creation of systems and means for preventing unsanctioned access to information being processed and special attacks causing the distortion, damage or destruction of data as well as alteration of the normal operating modes of informatization and communication systems and means;

- identification of technical devices and programs that pose a danger to the normal functioning of information technology systems, the prevention of information interception via technical channels, use of cryptographic means to protect information during its storage, processing and transmission via communication channels, and control over the fulfillment of special information protection requirements;

- certification of means of information protection, licensing of activities in the field of state secrets protection, standardization of information protection methods and tools;

- improvements in the system of certification of telecommunications hardware and software for automated information processing systems in terms of information security requirements;

- control over personnel actions in protected information systems and the training of personnel in the field of ensuring the information security of the Russian Federation;

- formation of the system of monitoring the indicators and characteristics of the information security of the Russian Federation in the most important spheres of life and activity of society and the state.

The economic methods for ensuring the information security of the Russian Federation include:

- the development of national information security programs and determination of the procedure for their financing;

- improvements in the system of financing for efforts to implement the legal and organizational-technical methods for information protection and the creation of the system of insurance of information risks of natural and legal persons.

6. Features of assurance of the information security of the Russian Federation in different areas of public life

The information security of the Russian Federation is one of the ingredients of the national security of the Russian Federation and exerts influence on the degree of protection of its national interests in different spheres of activity by society and the state. The threats to and methods for ensuring national information security are common to these spheres.

Each of them has its own specifics of ensuring information security, deriving from the specifics of security assurance facilities and their degree of vulnerability in respect of threats to the information security of the Russian Federation. In every sphere of activity by society and the state use can be made of private methods and forms determined by the specifics of the factors influencing the state of national information security in tandem with general methods for ensuring the information security of the Russian Federation.

In the economy sphere – Ensuring the information security of the Russian Federation in the economy sphere plays a key role in ensuring its national security.

The following are most susceptible to national information security threats **in the economy sphere**:

- the system of state statistics;

- the financial and credit system;

- automated information and accounting systems of subdivisions of federal executive bodies ensuring the activities of society and the state in the economy sphere;

- systems of financial accounting of enterprises, institutions and organizations under whatever form of ownership;

- systems of gathering, processing, storage and transmission of financial, stock exchange, tax, customs information and information on the foreign economic activity of the state as well as of enterprises, institutions and organizations under whatever form of ownership.

The transition to market relations in the economy has brought about the appearance in the Russian internal goods and services market of a multitude of national and foreign commercial structures: information and informatization and information protection tool producers and consumers. Uncontrolled activity by these structures in developing, manufacturing and protecting the systems of gathering, processing, storage and transmission of statistical, financial, stock exchange, tax and customs information creates a real threat to the security of Russia in the economy sphere. Similar threats arise with the uncontrolled attraction of foreign firms to creating such systems, as in this case favorable conditions take shape for unsanctioned access to confidential economic information and for monitoring its transfer and processing by foreign special services.

The critical state of enterprises of the national industries developing and manufacturing informatization, telecommunications, communication and information protection tools leads to extensive use of the relevant imported tools, which creates a danger of origination of Russian technological dependence on foreign states.

Computer crimes involving penetration by criminal elements into computer systems and networks of banks and other credit organizations pose a serious threat to the normal functioning of the economy as a whole.

The insufficiency of the legal and regulatory base that determines the liability of business entities for the unauthenticity or concealment of data on their commercial activities, on the consumer properties of the goods and services they produce, on the results of their economic activity, on their investments and so on hinders the normal functioning of the business entities. On the other hand, business entities may suffer substantial economic damage as a result of the divulgence of trade secrets information. In the systems of gathering, processing, storage and transmission of financial, stock exchange, tax and customs information the most dangerous are the illegal copying of information and its distortion as a consequence of deliberate or inadvertent violations of the technology for handling, and unsanctioned access to information. This also concerns the federal executive bodies engaged in the formation and distribution of information on the foreign economic activity of the Russian Federation.

The principal measures for ensuring the information security of the Russian Federation in the economy sphere are as follows:

- organizing and exercising state control over the creation, development and protection of systems and tools for gathering, processing, storage and transmission of statistical, financial, stock exchange, tax and customs information;

- radical restructuring of the system of state statistical reports so as to ensure the authenticity, completeness and security of information, carried out by introducing strict legal responsibility of officials for the preparation of primary information, organizing control over these officials' activities and those of statistical information processing and analysis services and restricting the commercialization of such information;

- development of national certified tools for information protection and their introduction in systems and tools for the gathering, processing, storage and transmission of statistical, financial, stock exchange, tax and customs information;

- development and introduction of national protected electronic payment systems on the basis of smart cards, electronic money and electronic commerce systems, the standardization of these systems and the elaboration of a legal and regulatory base governing their use;

- improvement of the legal and regulatory base governing information relations in the economy sphere;

- streamlining the methods of selection and training of personnel for work in economic information gathering, processing, storage and transmission systems.

In the domestic policy sphere – The most important Russian information security targets in the domestic policy sphere are:

- the constitutional rights and freedoms of man and the citizen;

- the constitutional system, national harmony, the stability of state authority, the sovereignty and territorial integrity of the Russian Federation;

- the open information resources of federal executive bodies and the mass media.

The following threats to the information security of the Russian Federation pose the greatest danger **in the domestic policy sphere**:

- violation of the constitutional rights and freedoms of citizens that are realized in the information sphere;

- insufficient legal governance of relations in the area of the rights of different political forces to use the media for the advocacy of their ideas;

- the spread of disinformation about the policy of the Russian Federation, the activities of the federal bodies of state authority and events occurring in the country and abroad;

- activities by public associations, aimed at a forcible change of the foundations of the constitutional system and seeking to disrupt the integrity of the Russian Federation, foment social, racial, national and religious strife and spread these ideas in the media.

The principal measures for ensuring the information security of the Russian Federation in the domestic policy sphere are:

- establishing a system for countering the monopolization of components of the information infrastructure by domestic and foreign entities – including the market for information services and the mass media;

- stepping up counterpropaganda activities aimed at preventing negative consequences of the spread of disinformation about Russian domestic policy.

In the foreign policy sphere – The most important Russian information security targets in the foreign policy sphere are:

- the information resources of the federal executive bodies implementing Russian Federation foreign policy, of the Russian representations and organizations abroad and the representations of the Russian Federation at international organizations;

- the information resources of the representations of the federal executive bodies implementing Russian Federation foreign policy on the territory of the constituent entities of the Russian Federation;

- the information resources of the Russian enterprises, institutions and organizations subordinate to the federal executive bodies implementing Russian Federation foreign policy;

- the blocking of the activities of Russian media in explaining to foreign audiences the goals and major thrust areas in the Russian Federation's state policy and its view of socially significant events in Russian and international life.

Among external threats to Russian information security **in the foreign policy sphere** those representing the greatest danger are:

- informational influence that foreign political, economic, military and information entities may have on the elaboration and implementation of the foreign policy strategy of the Russian Federation;

- disinformation being spread overseas about the foreign policy of the Russian Federation;

- violation of the rights of Russian citizens and legal entities in the information sphere abroad;

- attempts at unsanctioned access to information or attack attempts against information resources and the information infrastructure of the federal executive bodies implementing Russian Federation foreign policy, of Russian representations and organizations abroad and the representations of the Russian Federation at international organizations.

Among internal threats to Russian information security **in the foreign policy sphere** those representing the greatest danger are:

- violation of established information gathering, processing, storage and transmission procedures in the federal executive bodies implementing Russian Federation foreign policy and their subordinate enterprises, institutions and organizations;

- the information and propaganda activities of political forces, public associations, media and individuals distorting the strategy and tactics in the foreign policy activity of the Russian Federation;

- insufficient provision of information to the public on the foreign policy activity of the Russian Federation.

The principal measures for ensuring the information security of the Russian Federation in the foreign policy sphere are:

- elaboration of the main thrusts of state policy in the field of improving information support to the foreign policy course of the Russian Federation;

- development and realization of a set of measures to reinforce the information security of the information infrastructure of the federal executive bodies implementing Russian Federation foreign policy, of Russian representations and organizations abroad and the representations of the Russian Federation at international organizations;

- the creation for Russian overseas representations and organizations of conditions for work on the neutralization of the disinformation being spread there about the foreign policy of the Russian Federation;

- perfecting the information support of the work on counteracting abuses of the rights and freedoms of Russian citizens and legal entities abroad;

- better information support to the constituent entities of the Russian Federation with respect to foreign policy activity issues that fall within their competence.

In the field of science and technology – The most important Russian information security targets in the science and technology field are:

- fundamental, exploratory and applied research results potentially important for the techno-scientific, technological and socioeconomic development of the country, including information whose loss may inflict damage upon the national interests and prestige of the Russian Federation;

- discoveries, unpatented technologies, industrial designs, useful models and experimental equipment;

- scientific and technical cadres and the system for their training;

- management systems for integrated research complexes (nuclear reactors, particle accelerators, plasma generators, and others).

The following are principal categorizable external threats to Russian information security **in the field of science and technology**:

- the striving of developed foreign states to get illegal access to scientific and technical resources of Russia in order to use the results obtained by Russian scientists in their own interests;

- the creation of preferential conditions for foreign techno-scientific products in the Russian market and a simultaneous striving by developed countries to limit the development of Russia’s techno-scientific potential (buying up shares of advanced enterprises with their subsequent refocusing, keeping export and import restrictions and so on);

- the policy of western countries aimed at further destroying the unified techno-scientific space inherited from the USSR, of the member states of the Commonwealth of

Independent States through refocusing onto western countries their scientific and technical ties as well as individual, most promising scientific collectives;

- the step-up of activity by foreign state and commercial enterprises, institutions and organizations in the field of industrial espionage with the enlistment of intelligence and special services in it.

The following are principal categorizable internal threats to Russian information security **in the field of science and technology**:

- the lingering complicated economic situation in Russia, leading to a sharp drop in the financing of scientific and technical activities, a temporary decline in the prestige of the techno-scientific sphere and the outflow of ideas and advanced developments;

- the inability of national electronic industry plants to produce on the basis of newest microelectronics achievements and advanced information technologies competitive science-intensive products helping provide a sufficient level of Russian technological independence from foreign countries, which necessitates wide use of import hardware & software in setting up and advancing the information infrastructure in Russia;

- the serious problems in the field of patent protection of the results of scientific and technical activities of Russian scientists;

- the difficulties in carrying out information protection measures, especially in corporatized enterprises and in techno-scientific institutions and organizations.

The real way to counteract information security threats to the Russian Federation in the field of science and technology is to streamline national legislation governing relations in this sphere, and the implementation mechanisms for it. Toward this end the state must promote the creation of a system for assessment of likely damage from the realization of threats to the most important Russian information security facilities in the field of science and technology, including public research councils and independent expertise organizations working out recommendations for the bodies of state authority, both federal and in the constituent entities of the Federation, on the prevention of illegal or ineffective use of Russia's intellectual potential.

In the sphere of spiritual life – Ensuring national information security in the sphere of spiritual life aims to protect the constitutional rights and freedoms of man and the citizen associated with the development, formation and behavior of the individual, with freedom of mass information and use of the cultural, spiritual and moral legacy, historical traditions, and the norms of social life, with the preservation of the cultural wealth of all of Russia's peoples and with the realization of constitutional restrictions on human and civil rights and freedoms in the interests of keeping up and strengthening the moral values of society, the traditions of patriotism and humanism, the health of citizens, the cultural and scientific potential of the Russian Federation and of ensuring the nation's security and defense capabilities.

The most important Russian information security targets **in the sphere of spiritual life** are:

- the dignity of the person, freedom of conscience, including the right freely to choose, possess and disseminate religious or other beliefs, and to act in conformity with them, freedom of thought and speech (with the exception of propaganda or campaigning inciting

social, racial, national or religious hatred and strife) and the freedom of literary, artistic, scientific, technical and other kinds of creation and of teaching;

- the freedom of mass information;

- the inviolability of private life, personal and family privacy;

- the Russian language as a factor of spiritual unity of the peoples of multinational Russia and the language of interstate communication among the peoples of the member states of the Commonwealth of Independent States;

- the languages, moral values and cultural legacy of the peoples and nationalities of the Russian Federation;

- items of intellectual property.

The greatest danger in the sphere of spiritual life is the following **threats to the information security** of the Russian Federation:

- a deformation of the system of mass information owing to media monopolization as well as to uncontrolled expansion of the foreign media sector in the national information space;

- deteriorated condition and a gradual decline of Russian cultural heritage items, including archives, museum stocks, libraries, and architectural monuments, in view of insufficient funding for the relevant programs and activities;

- a possible disturbance of social stability, the infliction of harm upon the health and life of citizens as a result of activities by religious associations preaching religious fundamentalism as well as by totalitarian religious sects;

- foreign special services' use of media operating within the Russian Federation to inflict damage to the nation's security and defense capability and to spread disinformation;

- the inability of contemporary Russian civil society to ensure the formation in the growing generation, and maintenance in society, of socially required moral values, patriotism and civic responsibility for the destiny of the country.

The principal measures for ensuring the information security of the Russian Federation in the sphere of spiritual life are:

- the development in Russia of the foundations of civil society;

- providing economic and social conditions for the conduct of creative activity and the functioning of cultural establishments;

- elaborating civilized forms and methods for public control over the formation in society of spiritual values meeting the national interests of the country and over the education of patriotism and civic responsibility for its destiny;

- streamlining the Russian Federation legislation governing relations in the field of constitutional restrictions on human and civil rights and freedoms;

- government support of the measures to preserve and revive the cultural heritage of the peoples and nationalities of the Russian Federation;

- the formation of institutional mechanisms for ensuring the constitutional rights and freedoms of citizens and boosting their legal culture in the interests of countering deliberate or unintentional violations of these constitutional rights and freedoms in the sphere of spiritual life;

- the formation of effective legal and organizational mechanisms of access by media and citizens to open information about the activities of federal bodies of state authority or public associations, along with the assurance of the trustworthiness of data on socially significant events of public life being circulated via mass media;

- the development of special legal and organizational mechanisms for preventing illegal informational and psychological influences on the mass consciousness of society or uncontrolled commercialization of culture and science, along with similar mechanisms to ensure preservation of the cultural and historical values of the peoples and nationalities of the Russian Federation and rational utilization of the information resources amassed by society that constitute national property;

- the imposition of a ban on the use of electronic media airtime for the distribution of programs propagandizing violence, cruelty and antisocial behavior;

- counteracting the negative influence of foreign religious organizations and missionaries.

In the national information and telecommunication systems: The most important Russian information security targets in the national information and telecommunication systems are:

- information resources containing data classified as state secrets, and confidential information;

- informatization systems and facilities (computer hardware, information-computer complexes, networks and systems), software (operational systems, database management systems, and other general and applied software), automated management systems, communication and data transmission systems for the receipt, processing, storage and transmission of limited-access information, and their informative physical fields;

- technical means and systems handling open information, but located in premises where limited access information is handled, as well as the premises themselves designed for handling such information;

- premises designed for confidential negotiations, and negotiations in the course of which limited access information is announced.

The following are principal threats to the information security of the Russian Federation **in the national information and telecommunication systems**:

- the activities of special services of foreign states, and criminal confederations, organizations or groups and unlawful activities of individuals, aimed at obtaining

unsanctioned access to information and at monitoring the functioning of such information and telecommunication systems;

- use of import hardware/software in setting up and advancing information and telecommunication systems, necessitated by the objective lag of national industry in this area;

- violation of the established regulations for information gathering, processing and transmission, deliberate actions or errors by staff of the information and telecommunication systems, and hardware malfunctions or software failures therein;

- use of uncertified informatization and communication systems and tools with respect to security requirements, as well as of tools for information protection and for the control of their effectiveness;

- the enlistment in work on the creation, development and protection of information and telecommunication systems of organizations and firms not having state licenses for this kind of activities.

T**he major thrust areas** for information security efforts in the national information and telecommunications systems are:

- preventing interception of information from offices and facilities as well as of information transmitted via communication channels by technical means;

- the exclusion of unsanctioned access to information stored or being processed in the technical facilities;

- the prevention of technical-channel information leaks arising when operating the facilities for its processing, storage and transmission;

- the prevention of special hardware & software attacks resulting in the distortion, damage or destruction of information or failures in the operation of informatization facilities;

- information security arrangements when connecting national information/telecommunication systems to external information systems, including international;

- ensuring the security of confidential information during the interactions between information and telecommunication systems with varying classes of protection;

- the detection of electronic communication intercepting devices planted at facilities or in technical means.

The principal organizational and technical measures to protect information in the national information and telecommunication systems are:

- licensing for activities by organizations in the realm of information protection;

- attestation of informatization project compliance with information protection requirements when carrying out work involving use of data that constitute state secrets;

- certification of tools for information protection and for the control of their effectiveness as well as the protection of information against leaks via technical channels of informatization and communication systems and facilities;

- the imposition of territorial, frequency, energy, spatial and time restrictions in the utilization modes for technical means subject to protection;

- the development and application of protected information and automatic management systems.

In the defense sphere – The national information security targets in the defense sphere include:

the information infrastructure of the central military control agencies and of the military control agencies of the fighting services of the Russian Armed Forces, of the fighting arms, formations, large units, troop units and organizations within the Armed Forces and of the scientific research institutions of the Russian Ministry of Defense;

- the information resources of defense sector plants and of the scientific research institutions fulfilling state defense orders or concerned with defense problems;

- hardware & software for automated and automatic troop and arms control systems and for weapons and military equipment fitted with means of informatization;

- the information resources, communication systems and the information infrastructure of other forces, troop units and agencies.

External threats representing the greatest danger to Russian information security facilities in the defense sphere are:

- all kinds of intelligence activity on the part of foreign states;

- informational and technical influences (including electronic attacks, penetration into computer networks) by likely adversaries;

- subversive and sabotage activities by special services of foreign states, carried out by methods of informational and psychological influence;

- the activities of foreign political, economic and military entities directed against the interests of the Russian Federation in the defense sphere.

The internal threats representing the greatest danger to those facilities are:

- violation of the established regulations for the gathering, processing, storage and transmission of information held by headquarters and organizations of the Russian Ministry of Defense and by defense sector plants;

- deliberate actions or errors by staff of the special purpose information and telecommunication systems;

- unreliable functioning of special purpose information and telecommunication systems;

- possible information and propaganda activities undermining the prestige of the Russian Armed Forces and their combat readiness;

- the unsettledness of issues in the protection of the intellectual property of defense sector plants, resulting in the outflow of valuable government information resources abroad;

- the unsettledness of issues in the social protection of servicemen and members of their families.

The internal threats listed here will represent a special danger in conditions of an exacerbation of the military-political situation.

The major specific thrust areas in streamlining the Russian information security system in the defense sphere are:

- systematic identification of threats and their sources, the structuring of information security targets in the defense sphere and the determination of appropriate practical tasks;

- carrying out the certification of general and special software, applied program packets and information protection tools in the existing and projected military-purpose automated control systems and communication systems incorporating elements of computer equipment;

- continuous improvement of the tools for the protection of information against unsanctioned access, the development of protected communication and troop and arms control systems, the reliability upgrading of special software;

- structural improvement of the functional agencies of the information security system in the defense sphere and coordination of their mutual activities;

- improvement of the ways and means of providing strategic and operational camouflage and conducting intelligence and electronic countermeasures, along with the betterment of methods and tools for actively countering propaganda, information and psychological operations by a likely adversary;

- the training of information security experts in the defense sphere.

In the law enforcement and judicial spheres – The most important information security facilities in the law enforcement and judicial spheres include:

- the information resources of the federal executive bodies realizing law enforcement functions, judicial bodies, their information computer centers, scientific research and educational institutions containing special information and data of a confidential nature;

- information computer centers, their information, technical, program and normative support;

- information infrastructure (information computer networks, control posts, communication centers and lines).

External threats representing the greatest danger to information security facilities in the law enforcement and judicial spheres are:

- intelligence activities by special services of foreign states and by international criminal confederations, organizations and groups involving the gathering of information that reveals the objectives, activity plans, technical equipment, methods of work and places of deployment of special units and interior bodies of the Russian Federation;

- activities by foreign state and private commercial entities seeking to get unsanctioned access to information resources of law enforcement and judicial bodies.

Internal threats representing the greatest danger to the said facilities are:

- violation of the established regulations for the gathering, processing, storage and transmission of information held in files and automated databanks and used for crime investigation;

- insufficient legislative and normative regulation of the exchange of information in the law enforcement and judicial spheres;

- the lack of a unified methodology for the gathering, processing and storage of information of an investigative, reference, criminalistic and statistical nature;

- hardware malfunctions and software failures in the information and telecommunication systems;

- deliberate actions, and errors of staff directly engaged in creating and maintaining files and automated databanks.

Along with the widely used general methods and tools of information protection, specific methods and tools for ensuring information security in the law enforcement and juridical spheres are also applied.

Chief among them being:

- the creation of a protected multilevel system of integrated databanks of an investigative, reference, criminalistic and statistical nature on the basis of specialized information technology systems;

- upgrading the level of professional and special training of information system users.

In the conditions of emergency situations – The most vulnerable information security facilities in the Russian Federation in the conditions of emergency situations are the disaster relief and emergency response decision making system, and the system for the gathering and processing of information on the likelihood of emergency situations.

Of special importance to the normal functioning of the said facilities is the assurance of national information infrastructure security in the event of accidents, disasters and calamities. The concealment, receipt in delay, distortion or destruction of operational information, and unsanctioned assess to it by individuals or groups of individuals may lead to a loss of human lives as well as to the origination of different kinds of complexities in the elimination of the consequences of an emergency situation deriving from the specificities of informational influence under extreme conditions; to setting in motion large masses people

experiencing psychic stress; and to a quick rise and spread of panic and commotion among them on the basis of rumors and false or untrustworthy information.

In respect of these conditions, the specific thrust areas for efforts to ensure information security include:

- the development of an effective system of monitoring the objects of enhanced potential danger, whose disruption may cause emergency situations, and of forecasting emergency situations;

- the improvement of the system by which the public is informed about the dangers of outbreak of emergencies and about the conditions of their origination and development;

- enhancing the reliability of the information processing and transmission systems ensuring the activities of federal executive bodies;

- prediction of the behavior of the population under the influence of false or untrustworthy information about possible emergency situations and the elaboration of measures to help large masses of people in the conditions of these situations;

- the development of special measures for the protection of the information systems ensuring management of environmentally dangerous and economically important enterprises.

7. International cooperation by the Russian Federation in the realm of information security

International cooperation by the Russian Federation in the realm of information security is an integral part of political, military, economic, cultural, and other interactions among the countries which form the world community. Such cooperation must help enhance the information security of all members of the world community, including the Russian Federation.

A feature of international cooperation by the Russian Federation in the realm of information security is that it occurs in the conditions of toughened international competition for technological and information resources and for market dominance, coupled with continued attempts at creating a structure of international relations based on unilateral solutions to key problems in world politics, at resisting the consolidation of Russia’s role as one of the influential centers in an emerging multipolar world, at increasing the technological edge of leading world powers and at building up their capabilities to create the “information weapon.” All of this may lead to a new stage of the arms race in the information sphere and to the mounting danger of spying and operational technical penetration into Russia by foreign intelligence services, particularly with the use of the global information infrastructure.

The major thrust areas for international cooperation by the Russian Federation in the realm of information security are:

- prohibiting the development, spread and use of the “information weapon”;

- securing the international exchange of information, including information flows via national telecommunication and communication channels;

- coordination of computer crime prevention activities by law enforcement agencies of the countries which form the world community;

- prevention of unsanctioned access to confidential information in international banking telecommunication networks and world trade information support systems and to information of international law enforcement organizations waging a struggle against transnational organized crime, international terrorism, the spread of narcotic drugs and psychotropic substances, the illegal trade in arms and fissile material, and human trafficking.

In maintaining international cooperation by the Russian Federation in the realm of information security, special attention should be paid to problems of interaction with the member states of the Commonwealth of Independent States.

For this cooperation to be accomplished in the aforesaid major areas the active participation of Russia should be ensured in all the international organizations engaged in activities in the realm of information security, particularly in the field of the standardization and certification of informatization and information protection tools.

III. THE MAIN PROPOSITIONS OF RUSSIAN STATE INFORMATION SECURITY POLICY AND URGENT MEASURES TO REALIZE IT

8. The main propositions of Russian state information security policy

The RF state information security policy defines the main thrusts of activities to be pursued by the federal bodies of state authority and by the bodies of state authority of the constituent entities of the Russian Federation in this field, the procedure for assigning their responsibilities in protecting the interests of the Russian Federation in the information sphere within the thrust areas and rests on the observance of a balance of interests among the individual, society and the state in the information sphere.

The RF state information security policy is based on the following main principles:

- observance of the Russian Federation Constitution and laws and of the generally recognized principles and norms of international law in carrying out activities to ensure national information security;

- openness in realizing the functions of the federal bodies of state authority, the bodies of state authority of the constituent entities of the Russian Federation and public associations, that envisages the provision of information to the public about their activities with regard for the restrictions established by the legislation of the Russian Federation;

- the legal equality of all participants in the information interaction process regardless of their political, social or economic status, predicated on the constitutional right of citizens freely to seek, get, transmit, produce and disseminate information in any legal way;

- priority boost for modern RF information and telecommunication technologies, the production of hardware and software capable of ensuring the improvement of national

telecommunication networks, and their connection to global information networks with a view to the observance of Russia's vital interests.

The state in the course of the realization of its functions of ensuring the information security of the Russian Federation:

- carries out an objective and comprehensive analysis and prediction of threats to the information security of the Russian Federation, and works out measures for its assurance;

- organizes work of the legislative (representative) and executive bodies of state authority of the Russian Federation to implement a set of measures aimed at preventing, repulsing and neutralizing threats to national information security;

- supports the activities of public associations aimed at providing objective information to the population about socially significant events of public life and protecting society against distorted and untrustworthy information;

- exercises control over the design, manufacture, development, use, export and import of information protection tools by means of their certification and the licensing of activities in the field of information protection;

- pursues a requisite protectionist policy toward informatization and information protection tool producers within Russia, and takes measures to protect the domestic market against the penetration of inferior informatization tools and information products into it;

- facilitates granting access to world information resources and global information networks for natural and legal persons;

- articulates and implements Russia's state information policy;

- organizes development of a federal program to assure the information security of the Russian Federation combining the efforts of state and non-state organizations in this field;

- promotes the internationalization of global information networks and systems, and Russia's entry into the world information community on terms of an equal partnership.

Streamlining the legal mechanisms governing social relations arising in the information sphere is a priority thrust of state policy in the field of ensuring the information security of the Russian Federation.

This presupposes:

- effectiveness assessment of the application of current legislative and other normative legal acts in the information sphere, and elaboration of a program for their improvement;

- the establishment of institutional mechanisms for the assurance of information security;

- determining the legal status of all parties to relations in the information sphere, including information and telecommunication system users, and establishing their responsibility for the observance of the Russian Federation laws in this sphere;

- the creation of a system for the gathering and analysis of data on sources of threats to the information security of the Russian Federation, and on the implications of their accomplishment;

- the crafting of normative legal acts determining the organization of investigation and the procedure for judicial examination of illegal actions in the information sphere, and the rule on eliminating the consequences thereof;

- the elaboration of formal elements of a definition of law violations with regard for the specifics of criminal, civil, administrative and disciplinary liability, and the inclusion of the appropriate legal norms into the criminal, civil, administrative and labor codes and into the Russian Federation civil service laws;

- improvements in the system for the training of personnel used in the field of ensuring the information security of the Russian Federation.

Legal support to national information security should primarily be based on the observance of the principles of legality and of a balance of interests among citizens, society and the state in the information sphere.

The observance of the principle of legality requires that the federal bodies of state authority and those of the constituent entities should be strictly guided when resolving conflicts that may arise in the information sphere by the legislative and other normative legal acts governing relations in this sphere.

The observance of the principle of a balance of interests among citizens, society and the state in the information sphere presupposes legislative enshrinement of these interests in different areas of the functioning of society, and the use of forms of public control of the activities of the federal bodies of state authority and those of the constituent entities of the Russian Federation. Realizing the guarantees for the constitutional rights of man and the citizen concerning activities in the information sphere is a major task of the state in the realm of information security.

Elaborating the mechanisms of legal support to national information security includes measures to informatize the legal sphere as a whole.

To identify and harmonize the interests of the federal bodies of state authority, the bodies of state authority of the constituent entities, and other parties to relations in the information sphere and to craft requisite decisions, the state supports the formation of public councils, committees and commissions with broad representation of public organizations, and facilitates organizing their effective work.

9. Urgent Measures to Realize the State Information Security Policy of the Russian Federation

Urgent measures to realize the state information security policy of the Russian Federation are:

- the development and introduction of mechanisms to realize legal norms governing relations in the information sphere, and the preparation of a blueprint for legal support to national information security;

- the development and realization of mechanisms to raise the effectiveness of state guidance of state media activities and to implement state information policy;

- crafting and implementing federal programs aimed at the formation of generally accessible information resources archives of the federal bodies of state authority and of the bodies of state authority of the constituent entities, boosting the legal culture and computer literacy of citizens, developing the infrastructure of Russia's unified information space, counteracting information war threats in a comprehensive way, creating secure information technologies for systems used in the course of the realization of the vitally important functions of society and the state, suppressing computer crime, devising a special purpose information technology system in the interests of the federal bodies of state authority and of the bodies of state authority of the constituent entities, ensuring Russia's technological independence in the area of development and operation of information technology systems for defense purpose;

- developing the system for the training of personnel used in the field of ensuring the information security of the Russian Federation;

- harmonizing national standards in the area of informatization and the assurance of information security for automated management systems and general and special purpose information and telecommunication systems.

IV. THE ORGANIZATIONAL BASE OF THE SYSTEM OF ENSURING THE INFORMATION SECURITY OF THE RUSSIAN FEDERATION

10. The main functions of the system of ensuring the information security of the Russian Federation

The Russian Federation's information security system is designed for the implementation of state policy in this field.

The main functions of the national information security system are:

- the development of a legal and regulatory base in the realm of national information security;

- the creation of conditions for the realization of the rights of citizens and public associations to law-permitted activities in the information sphere;

- determining and maintaining a balance between the requirement of citizens, society and the state in a free exchange of information and indispensable restrictions on information dissemination;

- the assessment of the state of national information security, the identification of sources of internal and external information security threats, the determination of priority thrust areas for preventing, repulsing and neutralizing these threats;

- the coordination of activities of the federal bodies of state authority and other state bodies tackling the tasks in ensuring the information security of the Russian Federation;

- control of the activities of the federal bodies of state authority, the bodies of state authority of the constituent entities, and state and interagency commissions dealing with national information security concerns;

- prevention, identification and suppression of violations involving encroachments on the lawful interests of citizens, society and the state in the information sphere and on judicial proceedings relating to cases of crimes in this area;

- developing the national information infrastructure, and the industry of telecommunication and information tools, and improving their competitiveness in the domestic and foreign market;

- organizing the elaboration of federal and regional information security programs, and coordinating activities for their implementation;

- the pursuit of a unified technical policy in the realm of national information security;

- the organization of fundamental and applied research in the realm of national information security;

- the protection of government information resources, primarily in the federal bodies of state authority, the bodies of state authority of the constituent entities, and defense sector enterprises;

- control over the creation and use of information protection tools by mandatory licensing of activities in this area and the certification of information protection tools;

- the improvement and development of a unified system for the training of personnel used in the field of ensuring the information security of the Russian Federation;

- maintaining international cooperation in the realm of information security and the representation of the interests of the Russian Federation in the appropriate international organizations.

The remit of the federal bodies of state authority, the bodies of state authority of the constituent entities, and other state bodies which are part of the system (subsystems) of national information security is defined by federal laws and by normative legal acts of the President and Government of the Russian Federation.

The functions of the bodies coordinating the activities of the federal bodies of state authority, those of the constituent entities, and other state bodies within the system (subsystems) of national information security are defined by individual normative legal acts of the Russian Federation.

11. Main elements of the organizational base of the system of ensuring the information security of the Russian Federation

The Russian Federation’s information security system is a part of the security system of the country.

The RF national information security system is based on the delineation of powers among the legislative, executive and judiciary branches in this sphere, and of the terms of reference between the federal bodies of state authority and the bodies of state authority of the constituent entities of the Russian Federation.

The main elements of the organizational base of the national information security system are: President of the Russian Federation, Federation Council of the Federal Assembly of the Russian Federation, State Duma of the Federal Assembly of the Russian Federation, Government of the Russian Federation, Security Council of the Russian Federation, federal executive bodies, interagency and state commissions established by the President or Government of the Russian Federation, executive bodies of the constituent entities of the Russian Federation, bodies of local self-government, judicial bodies, public associations, and citizens participating in accordance with Russian Federation legislation in addressing national information security tasks.

The President of the Russian Federation directs within his Constitutional remit national information security agencies and forces; authorizes national information security actions; in conformity with Russian Federation legislation forms, reorganizes and abolishes national information security agencies or forces subordinate to him; and defines in his annual Federal Assembly addresses the priority thrust areas for state information security policy, and implementation measures for the present Doctrine.

The Chambers of the Federal Assembly of the Russian Federation form on the basis of the Constitution – and upon submission from the President or Government – a legislative base in the realm of national information security.

The Government of the Russian Federation within its remit and with regard for the national information security priorities articulated in the President's annual Federal Assembly addresses coordinates the activities of federal executive bodies and those of the constituent entities, and in shaping draft federal budgets for relevant years in a prescribed manner, envisages the allocation of necessary funds for implementing federal programs in this area.

The Security Council of the Russian Federation conducts work on the identification and assessment of national information security threats, operationally prepares draft Presidential decisions to prevent such threats, works out proposals for national information security arrangements, as well as proposals to specify individual provisions of the present Doctrine, coordinates the activities of national information security forces and agencies, and oversees the implementation of the relevant decisions of the President of the Russian Federation by the federal executive bodies and those of the constituent entities.

The federal executive bodies see to it that Russian Federation legislation and the decisions by the President and Government of the Russian Federation with respect to national information security are complied with; within their remit, develop normative legal acts in this field and submit them to the President and Government of the Russian Federation in a prescribed manner.

Interagency and state commissions set up by the President or Government of the Russian Federation tackle in line with the powers granted to them the tasks in ensuring the information security of the Russian Federation.

The executive bodies of the constituent entities interact with the federal executive bodies on compliance with Russian Federation legislation and with the decisions of the President and Government relating to national information security, as well as on federal program implementation in this field; in conjunction with bodies of local self-government carry out the measures to engage citizens, organizations and public associations in helping solve problems to assure national information security; and submit proposals to federal executive bodies on improving the system for ensuring the information security of the Russian Federation.

The bodies of local self-government ensure the observance of the legislation of the Russian Federation in the realm of national information security.

The judicial bodies administer justice in cases of crimes involving encroachments on the lawful interests of the individual, society or the state in the information sphere and provide the judicial protection of citizens and public associations whose rights were infringed in relation to their activities in assuring national information security.

The national information security system of the Russian Federation may include subsystems (systems) oriented on tackling local tasks in this sphere.

* * *

Implementing the urgent national information security measures listed in this Doctrine presupposes elaboration of an appropriate federal program. Concretization of certain Doctrine provisions applicable to individual areas of societal and state activity may be done in the respective documents approved by the President of the Russian Federation.