Sarichev N.V., Melnitchenko D.V.

External and internal threats
of information security of Russia

Information security is the security of information environment of the person, the society and the state from deliberate and unpremeditated threats and influences. Ensuring of information security of the Russian Federation is closely interconnected with decision of internal questions of the country: problems of political, economic, military, social and other kinds of national security. For ensuring of external aspect of information security the great role should be devoted to interaction with informational bodies of other countries.

***Key words:** counteraction to ideology of terrorism, information sphere, information threats, information security, protection from information and psychological threats.*

Information sphere of Russia is characterized by active development of modern means of information exchange and various types of computer systems. It creates conditions for ensuring of information support of activity of the State machinery at all levels and in all branches of the power.

At the same time weak attention given to problems of information security ensuring creates objective conditions for illegal access to closed information, its plunder or destruction. Possibility of manipulations with information for negative influence on the process of political decisions' making has special danger [1].

In the list of the threats' kinds of information security designated in the Doctrine [2], it is necessary to pay special attention to:

– exclusion of Russian news agencies, mass media, from internal information market and strengthening of dependence of spiritual, economic and political spheres of public life of Russia from foreign information structures;

– information's manipulation (misinformation, concealment or distortion of information).

For Russia there are main aims of protection from information and psychological threats:

1) protection from destructive information and psychological influences of society environment, mentality of the population, social groups of citizens;

2) counteraction to attempts of manipulation of the population's information perception processes from hostile to Russia political forces spent with a view to easy the government's defensibility;

3) defending of national interests, purposes and values of Russia in information space (global, national, regional, subregional, countries of the UNC);

4) constant tracing of Russian society's relations to the major problems of national safety (diagnostics of public opinion, psychological state of the nation).

Now the world leading countries have powerful potential of information counteraction (first of all, the USA, China, Israel, France, Great Britain, Germany) which can

provide them the achievement of political and economic aims, especially when there are no international legal norms of conducting of information struggle.

In the Doctrine of information security of the Russian Federation there are defined the following basic sources of internal threats of information safety [2].

To internal sources they concern:

– critical condition of native industries;

– unfavorable criminal situation accompanied by the tendencies of merging of the state and criminal structures in information sphere, criminal structures' receptions of access to the confidential information, strengthening of influence of the organized crime on society's life, decrease of the degree of security of legitimate interests of citizens, society and state in information sphere;

– insufficient coordination of the federal State power bodies', State power bodies' of the subjects of the Russian Federation activity on formation and realization of the single state policy in the sphere of information security ensuring of the Russian Federation;

– insufficient elaboration of the standard legal base regulating relations in information sphere, and also insufficient practice of law application;

– lack of development of civil society's institutes and insufficient state control over development of information market of Russia;

– insufficient financing of arrangements for information security ensuring of the Russian Federation;

– insufficient economic power of the state;

– decrease of effectiveness of the education and upbringing system, insufficient quantity of qualified personnel in the sphere of information security ensuring;

– insufficient activity of federal State power bodies, State power bodies of the subjects of the Russian Federation in the society's informing on their activity, in explanation of decisions, in formation of the open state resources and development of the system of citizens' access to them;

– in comparison with the world leading countries, Russia's lack of development on the level of informatization of federal State power bodies, State power bodies of the subjects of the Russian Federation and bodies of local governments, credit and financial sphere, industry, agriculture, education, public health services, sphere of service and life of citizens.

In the internal policy sphere the greatest danger is represented by the following threats of information security of the Russian Federation:

– infringement of constitutional laws and freedom of citizens realized in information sphere;

– insufficient legal regulation of relations in the sphere of rights of various political forces to use of mass media for propagation of their ideas;

– distribution of misinformation about the Russian Federation policy, activity of the federal State power bodies, events occurring in the country and abroad;

– activity of public associations directed on violent change of bases of the constitutional system and infringement of integrity of the Russian Federation,

rousing of social, racial, national and religious hostility, on distribution of these ideas in mass media.

In the foreign policy sphere the greatest danger among the internal threats of the information security of the Russian Federation there represent:

−information and propaganda activity of political forces, public associations, mass media and persons, that deforms strategy and tactics of the foreign policy activity of the Russian Federation;

−population's insufficient knowledge of the foreign policy of the Russian Federation.

In the foreign policy sphere the greatest danger among the external threats of information security of the Russian Federation there represent:

−informational influence of foreign political, economic, military and information structures on development and realization of the strategy of the foreign policy of the Russian Federation;

−distribution of misinformation about the foreign policy of the Russian Federation abroad;

−infringement of the rights of the Russian citizens and juridical persons in informational sphere abroad;

−attempts of unapproved access to information and influences on information resources, information infrastructure of the federal State executive power bodies realizing foreign policy of the Russian Federation, Russian representations and organizations abroad, representation of the Russian Federation at international organizations [2].

On the basis of national interests of the Russian Federation in informational sphere they form strategic and current problems of internal and foreign state policy on the information security ensuring.

There are distinguished four basic components of national interests of the Russian Federation in informational sphere.

The first component of national interests of the Russian Federation in informational sphere includes observance of constitutional laws and freedom of the person and the citizen in the sphere of information reception and its use, ensuring of spiritual renovation of Russia, preservation and strengthening of society's moral values, traditions of patriotism and humanism, cultural and scientific potential of the country.

The second component of national interests of the Russian Federation in informational sphere includes the informational support of the state policy of the Russian Federation, connected with giving to Russian and international public of trustworthy information about the state policy of the Russian Federation, its official position on socially significant events of Russian and international life, with providing of the citizens' access to open state information resources.

The third component of national interests of the Russian Federation in informational sphere includes development of modern information technologies, native information industry, including the industry of informatization means, telecommunica-

tion and communication, providing requirements of home market with its production and exit of this production on the world market, and also providing of accumulation, safety and effective utilization of native information resources. In modern conditions only on this basis it is possible to solve the problems of creation of high technologies, technological reequipment of the industry, increase of achievements of native science and techniques. Russia should take a worthy place among the world leaders of the microelectronic and computer industry.

The fourth component of national interests of the Russian Federation in informational sphere includes protection of information resources against unapproved access, ensuring of information and telecommunication systems' safety, both already developed, and created on the territory of Russia [3].

According to A.U. Kiryanov [1], at the present stage of development of Russia in informational sphere, the primary aims on realization and protection of national interests are:

– Development and acceptance of the long-term program on providing of the exit on a level of the world leading countries in the sphere of creation of computer science and management systems, based on the newest information technology.

– Ensuring of freedom of information reception and distribution by citizens, other subjects of public relations in interests of formation of civil society, democratic lawful state, science and culture development.

– Ensuring of reliable protection of information potential of Russia (i.e. the whole complex of information, providing national interests of the country; systems of its reception, keeping, processing and distribution; its subjects) from its wrongful use to the detriment of interests of the person, society and the state protected by the law. Control over intellectual production's export and also informational databanks' export from the country. Organization of effective system of the personnel's preparation and retraining in information security ensuring sphere.

– Development of interaction of the state and nonstate systems of information support with a view to more effective utilization of information resources of the country.

– Perfection of the system of the standard and legal acts regulating property relations and observance of the balance of interests of personality, society and state in the sphere of formation, keeping and use of information resources. Formation and development of the federal and regional centers of certification of systems of information protection and their elements.

– Counteraction to purposeful actions on misinformation of the power, the country population, to use of information exchange channels for infringement of control systems by various spheres of state life activity.

– Creation of the general informational space of the UNC countries in interests of assistance to integration processes, increase of efficiency of interaction in realization of common interests. Inclusion of Russia in the international system of

information exchange with regard for ensuring of Russian national interests and counteraction to actions of information intervention.

‒ Ensuring of decisions' making on unconditional interdiction for use of the information weapon in a peace time at international level [1].

Further it is offered to concentrate attention on a role of the state in information protection sphere. Principal propositions on information protection are establishes by the Federal law "On information" (clause 16). The law considers information protection as a complex of "legal, organizational and technical measures directed on:

1) ensuring of information protection from illegal access, destruction, modifying, blockings, copying, granting, distributions, and also from other wrongful actions concerning such information;

2) observance of confidentiality of information of the limited access;

3) realization of the right to information access".

The last purpose has no relation to information protection at first sight. But it is not so. It is necessary to defend not only information of the limited access, but also open information, access to which should be unlimited. It is also the problem of the state concerning information given for general consideration by the State power bodies and local power bodies.

The following category of protected information is information of the limited access, being at any confidentiality mode. But the state role is basically various in different modes of ensuring.

Public information is necessary to be defended from blocking of access, destruction, modifying (distortion). Information of the limited access is necessary to be defended from destruction, modifying, illegal copying, divulging, illegal access, illegal use [4].

Considering the global character of the processes of informatization and occurrence of international cybercriminality, the world community should have interstate organizational structures for coordination of works in information safety sphere.

The main international body is the United Nations Organization and the Security Council created by it. These bodies coordinate states' efforts on realization of actions in information safety sphere and struggle against crimes in information technologies' sphere. Disputed questions are solved at International court at interstate level.

The system of information security ensuring of the Russian Federation is formed on the basis of differentiation of the legislative, executive and judicial power bodies of the federal level, level of the Russian Federation's subjects, departmental structures, and also services of enterprises and organizations.

Thus, in connection with the newest scientific and technical achievements in the sphere of computer science and information technologies, modern rivalry of the states and other objects of social nature is characterized by occurrence of a new factor – information. Through target influence on information environment threats of national safety in various spheres of human activity are realized. In the political sphere the increasing importance there gets information and psychological influence with a view

to form relations in society, its reaction to occurring processes. In the economic sphere there grows vulnerability of economic structures from unauthenticity, delay and illegal use of economic information. In the military sphere an outcome of the armed struggle depends more and more on quality of extracted information and a level of development of information technologies on which there are based systems of intelligence service, radio-electronic struggle, management of armies and of high-precision weapon. In the sphere of spiritual life in society there is a danger of development of aggressive consumer ideology, distribution of ideas of violence and intolerance and other negative influences on consciousness and mentality of the person by means of electronic mass media. Information environment, being a system forming factor in all kinds of national safety (political, economic, military, etc.), at the same time is an independent object of protection.

References
1. Kiryanov A.U. Essence of information aspect of national security of the Russian Federation // International public and private law. – 2005. – # 3. – P. 42.
2. The doctrine of information security of the Russian Federation, confirmed by the President of the Russian Federation of 9/9/2000 # Pr-1895 // Russian newspaper. – # 187. – 2000.
3. Kovaleva N.N. Information right of Russia: the manual. – M: Publishing and trading corporation "Dashkov and C", 2007. – P. 234.
4. Volchinskaya E.K. Role of the state in information security ensuring // Information right. – 2008. – # 4. – P. 9–16.
5. Rodichev U.A. Information security: standard and legal aspects: the manual. – SPb.: Peter, 2008. – P. 86–87.