INNOVATIVE DEVELOPMENT OF TOOLS AND TECHNOLOGIES TO ENSURE THE RUSSIAN INFORMATION SECURITY AND CORE PROTECTIVE GUIDELINES

Maximov R.V.[1], Krupenin A.V.[2], Sharifullin S.R.[3], Sokolovsky S.P.[4]

In this work, we produced the analysis results of information technology development and information security threats in various areas. Effective use information technologies is a core factor for accelerating economic development and organizing new information society. However, information technology evolution is limited by capabilities of information security tools, their extensive development and ever-growing threats. The existing autocratic control of the information security system leads to the inevitable introduction of bans on technologies and infrastructures not controlled by it, that in turn reduces the effectiveness of innovation activities in the field of information technologies. Contradictions between the growth of information technology applications by business entities and the achievement of an acceptable level of their information security are shown. It is shown that intelligence tools and an effective information security system are in constant antagonistic conflict that can be described by a zero-sum pair game, and there is a tendency for advanced technical development of intelligence systems and tools in relation to the information security system. The possible ways for innovative development of information security tools and technologies are produced. This tools and technologies implementing principle of non-conflict protection.

Keywords: *information technologies, information threats, information structure, basic protective settings.*

DOI: *10.21681/2311-3456-2019-1-10-17*

Introduction

During evolution of information technologies and the infrastructure gaining global cross-border character there are negative processes generating threats of national security of the state in economic, defensive, information and other spheres [1]. It is shown that the effective use of information technologies in all fields of activity of the personality, societies and the state which is a factor of acceleration of economic development and formation of information society is considerably limited to opportunities of means of ensuring of information security, their extensive development causing considerable technological lag from innovations in the sphere of information technologies [2, 3]. The existing autocratic control of a system of ensuring information security leads to inevitable decrease in efficiency of innovative activity in the sphere of information technologies.

Information threats and ways to overcome them

Among the complex problems, accompanying processes of reforming of social and economic policy of the Russian Federation, national security issues in the information sphere have gained paramount significance in recent years. In this regard the Doctrine of Information Security of the Russian Federation[5] notes that the main information threats caused by globalization and cross-border character of information technologies and infrastructures are caused by (see Fig. 1):

possibilities of foreign information and technical impact on information infrastructure with military purposes;

activity of organizations which are carrying out technical investigation concerning the Russian public authorities, scientific organizations and enterprises of the defense industry;

use of information technologies for information and psychological impact on the population for the purpose of destabilization of a social and internal political situation, forcing of international tension;

growth of scale of crime in credit and financial sphere;

increase in the number of crimes related to violation of constitutional rights and freedoms of a person and citizen regarding to personal privacy, personal and family secret;

impossibility to realize based on the principles of confidence joint fair resource management to ensure the safe and sustainable functioning of the Internet.

Overcoming and preventing the above mentioned threats involves:

- improving information security system;
- innovative development of the information technology industry;

1 Roman Maximov, Dr.Sc. (in Tech.), Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: rvmaxim@yandex.ru

2 Alexander Krupenin Dr.Sc. (in Tech.), Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: a_krupenin@mail.ru

3 Sergey Sharifullin, Ph.D., Associate Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: SharifullinSR@mail.ru

4 Sergey Sokolovsky, Ph.D., Associate Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: ssp.vrn@mail.ru

5 www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

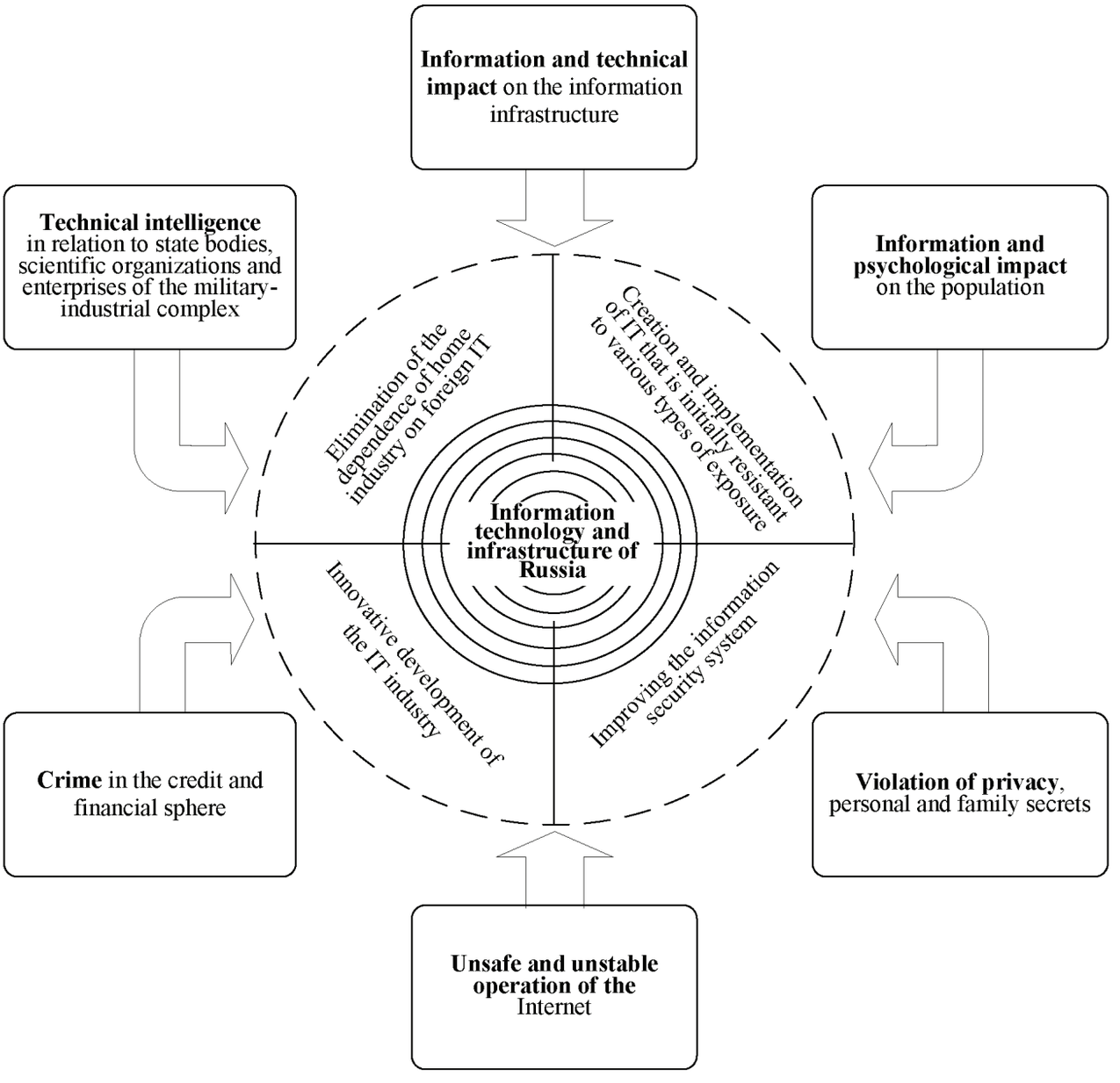

Fig. 1. Types of information threats and ways of their overcoming

- the elimination of domestic industry dependence on foreign information technologies;

- creation and implementation of the information technologies that are initially resistant to various types of impact.

The solution of these tasks serves to achieve national interests in the information sphere, and first of all to ensure the sustainable and smooth functioning of the information infrastructure of Russia.

But is there a hidden contradiction between the desire to effectively use information technologies for economic development and the formation of the information society which cause increasing in information needs of public authorities (business entities), and the capabilities of information security tools that are technologically lagging behind? It is necessary to consider the main features of the evolution of information technology, information infrastructure and information security tools, to link the basic concepts that characterize these features into conceptual schemes to respond to this issue.

The development of infocommunications in the 21st century is so intense that it is accepted to speak [4] about the information science and technology revolution, the result of which is a series of qualitative changes in social relations. More and more industries and sectors of the economy are focused on meeting the needs of officials for information services, which are growing in the face of shrinking management cycles. There is a reverse trend at the same time: forms of economic activity and public relations are changing under the influence of technology [5].

Tendencies of development of information infrastructure

The basis of the «explosive» development of information infrastructure elements is the achievements of «high» technologies in the areas of ultrahigh-level

cleaning of materials, the high-precision formation of integrated circuits elements and the introduction of high-tech components into the technical means that make up the information infrastructure. A common feature of «high» technologies is their critical dependence on each other leading to the spread of integration and convergence processes. Integration of telecommunication processes, devices, networks and services takes place by interpenetration and absorption. The relationship of the main trends and factors that determine the development of communication systems and networks, which constitute the material basis of the information infrastructure, is presented in Fig. 2. As a result of development of «high» technologies and growth of information needs of onsumers of information services life cycle of technical solutions – information technologies is reduced, and the range of information services increases.

strategic balance of forces in the world, but also change the existing criteria for assessing such a balance based on the correlation of geopolitical, economic and military factors. Control systems make it possible to implement political decisions with which only a very narrow circle of people agrees, and the number of people whose local actions can have global consequences (nuclear power plant operators, the chemical complex operators, financial structures, terrorists and extremists) has increased dramatically. The corridor of what humanity can afford without risking global catastrophic changes is very small: integrated distributed (global and cross-border) information technologies and infrastructures (see Fig. 3) have a wide range of features that are not inherent in the currently archaic dedicated (localized) communication systems and ACS.

An attacker, who carries out some combination of destructive effects from the entire arsenal of tools

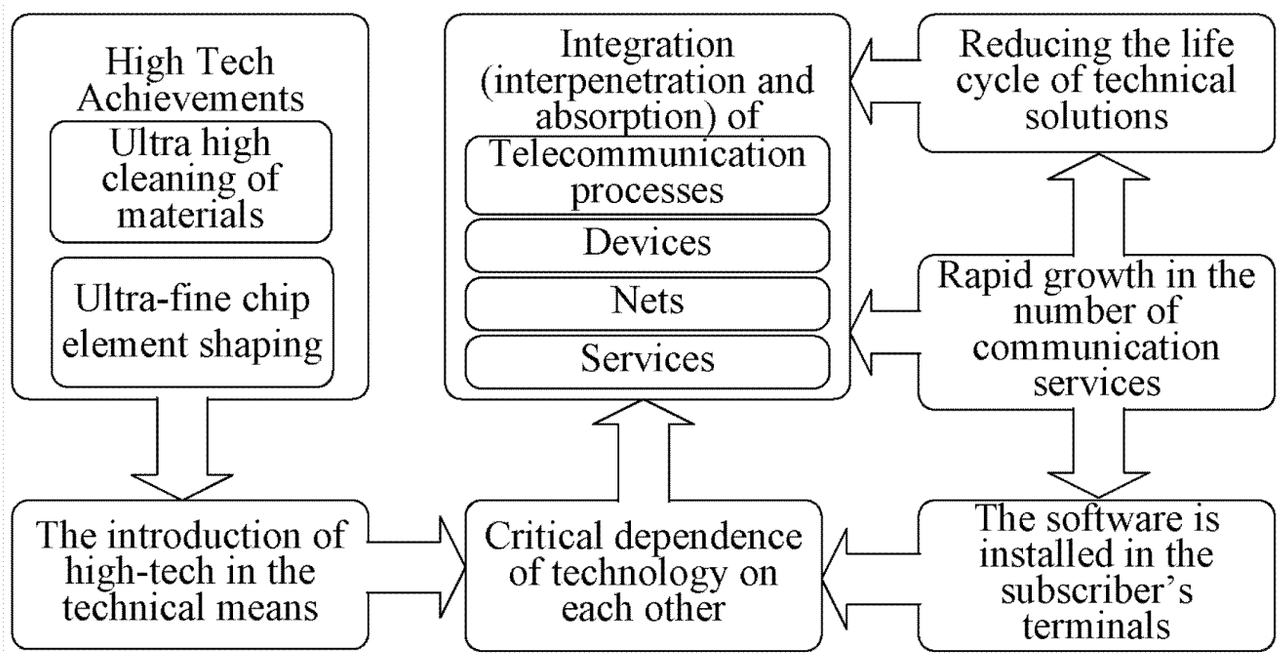

Fig. 2. The tendencies and factors defining development of information infrastructure

The software installed in terminal devices of subscribers, and the special «intellectual» networks intended to simplify realization of new services become a basis of information services.

As a result of the integration of communication and information technologies, the communications industry has been able to provide information services directly, forming the infocommunication infrastructure of the society, bringing traffic flows to the consumer of services in the future. Information owners act as the dominant social group of the society, which has got the name of the «global information society». The participation of any state in the processes of globalization is necessary for maintaining its status, acquiring and maintaining the required rates of economic development, and obtaining its share in world production and sales markets.

On the other hand, the rapid improvement of methods of targeted impact on information processes and control systems of the warring parties can not only influence the

available to him, seeks to influence the quality of decisions made by the opponent. For this purpose it realizes actions which it is possible to arrange conditionally in the range from interception of management of an information system (taking it under control) before its transfer to failure state (the so-called «denial of service»). The last phase is always obvious to the defending party and is far from always beneficial for the attacker, since, firstly, he compromises his actions, and, secondly, he loses his connection with the object of influence. In any case, a prerequisite for the implementation of the attacker's plans is the ability to monitor the state of the object of protection [6].

Such monitoring can be defined as a process aimed at obtaining information on the composition, structure, operation algorithms, location and ownership of an information system (technology), as well as data stored, processed and transmitted in it.

Monitoring is carried out by organizing and implementing dialogue (procedural) interaction with elements of the

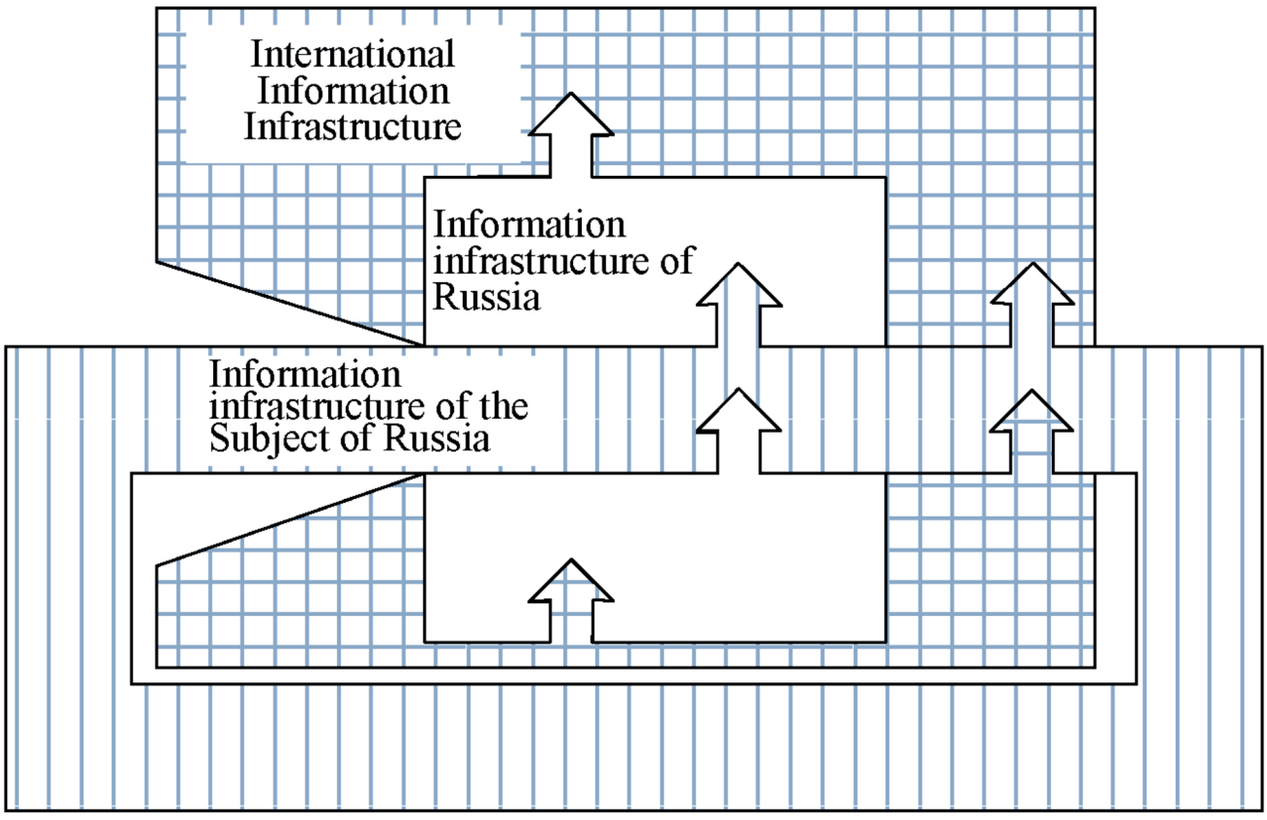

Fig. 3. The infrastructure of the subject of Russia integrated into global information infrastructure

information system (technology), which are characterized by undeclared capabilities, vulnerabilities and openness of the architecture [7, 8]. The groups controlling the activities of social networks (Twitter, Facebook) and users' mobile applications also act as an attacker.

The openness of the architecture and protocols leads to the possibility of interaction through the organization of the interfaces of the monitoring system with the elements of the information system (technology). It is the interfaces that allow the interaction of serially connected devices and programs of the derived aggregate system that implements the information leakage channel. Vulnerabilities lead to the possibility of organizing multiple channels of information leakage, and undeclared capabilities lead to the «delivery» of technical tools (bench marks) of monitoring to the infrastructure of an information system and ensuring contact with the object of protection.

Basic protective settings

The range of actions of the defender is potentially large. Countering the attacker is also subject to planning and has deep non-technological roots. It is connected with the fact that despite obvious opposition of technical systems, management of them has subject character. So-called basic defensive settings are known [9] (see Fig. 4).

The basic defensive settings are: distancing with the enemy, control of the influence channels and control of information flows. They are paired and can be of passive and active character. Active protection takes place only in cases where the danger emanates from another subject, whereas passive protection is applied in relation to factors of non-subject origin (to elements).

The use of the first setting provides an increase in the distance between opponents to secure borders. This setting implements the principle of spatial security. Archaic information infrastructures were isolated both topologically and by reducing the electromagnetic availability of the protected system to the enemy (passive form of protection). The evolution of infrastructures has led to their globalization and transboundary, therefore the construction of dedicated information infrastructures does not correspond to modern economic challenges and the desire to form an information society, and the active form – the destruction of the enemy – in the context of this article has such a specific and narrow scope that is not further considered.

The use of the second setting means the establishment of physical and logical obstacles with controlled characteristics to counter the enemy. This setting does not prevent the creation of global and cross-border infrastructures, but imposes on them implementation of a certain range of regulations, as sets of rules defining the procedure for working in this objective situation (passive form of protection). The active form – the removal of obstacles to impact on the opponent – is quite clearly embodied in the form of organizational and technical measures of influence on the subject-source of danger. However in the conditions of globalization of technologies and infrastructures identification of such subject is often difficult, impossible or does not enter competence (an arsenal of opportunities) of the concrete system of a specific information security system. In this case, the system

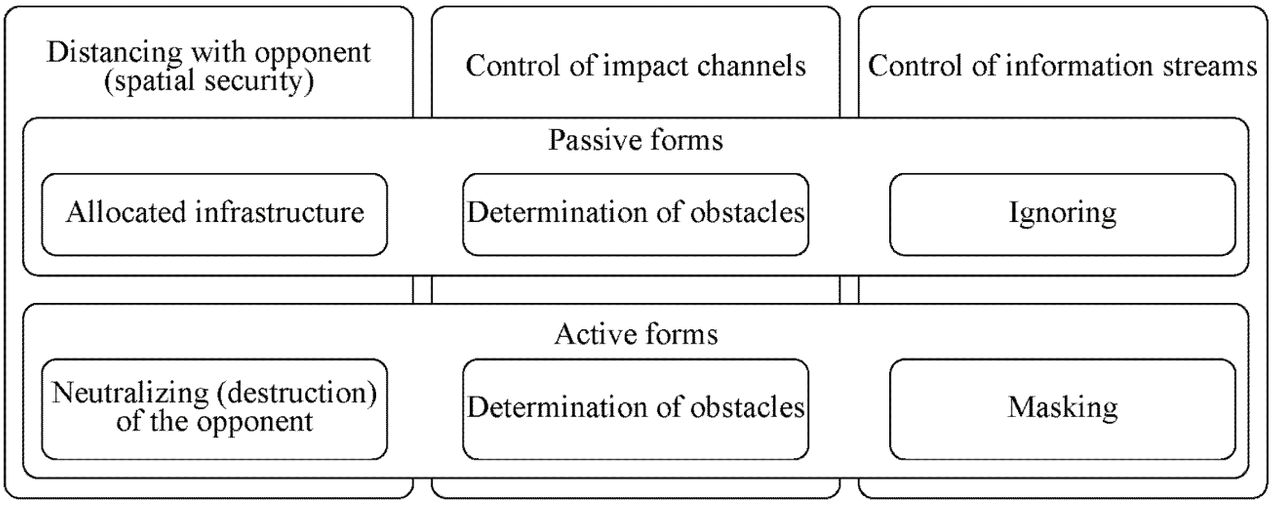

Fig. 4. Classification of basic protective settings

«assigns» the source of danger to the «element», and the entire responsibility for the fact, for example, of information and technical impact on the information infrastructure, is placed either on the shortcomings of the regulations or on their failure to be fulfilled by a specific user of information technology. The elimination of the lack of regulations is called the improvement of the information security system, and the elimination of the user fault – the personalization of responsibility for the failure to comply with the regulations. However, the failure of a particular user of an information technology or infrastructure to maintain information security regulations is often associated with a change (growth, evolution) of his information needs! Certainly there are applications [10] when such evolution is allowed only «in a planned order», but in article the ways of acceleration of economic development, formation of information society and innovative activity realized in the sphere of information technologies of broad application are considered. Obviously, the lack of regulations manifests itself just «on the spot»: first there is a threat, then (with a lag) a means of protection is erected against it – a set of organizational measures and technical ones implementing them. At this point, a new version of information technology is entering the market; information needs of users are changing (see Fig. 5).

Based on the analysis of the second protective setting, we can state that:

there is a tendency for advanced technical development of intelligence systems and facilities and information technology impacts (see Fig. 1) with respect to the information security system;

there is a technological lag in the means of ensuring information security from innovations in the field of information technologies;

the technical implementation of the updated regulations is based on the principle of proportionality of the protection elements to the information security threats identified at the previous step;

a variety of states which will be allowed by the updated regulations as safe will be less, than a potential variety of information technology of new generation.

In order to complete the analysis of opportunities of realization of the second basic protective installation at safety of information technologies and infrastructures, it is necessary to list briefly the main signs of the means of protection realizing this installation showing limitation of their effectiveness in the conditions accepted in article.

Such tools and methods of protection are built essentially on the basis of methods that implement a power

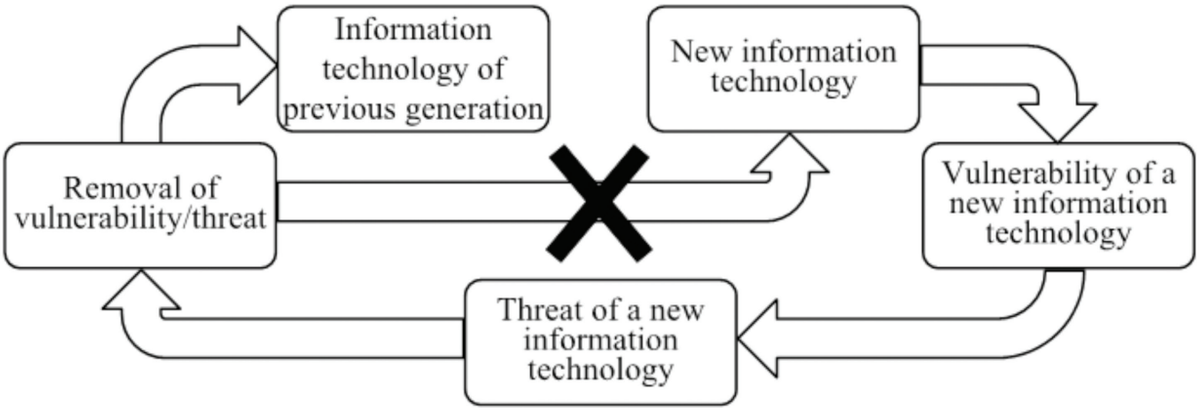

Fig. 5. To a question of technological lag of means of ensuring of information security from innovations in the sphere of information technologies

demonstrative blocking of access to information or channels of information leakage. The term «power» describes the «combat» potential of an element of the defense system, as opposed to the threat. The term «demonstrative» means the presence (clearly demonstrated) of an element and its potential (quality), which corresponds to the importance of the protected object and are additional features for an attacker who makes a decision about the importance of the protected object. Power demonstrative blocking of information is implemented by the creation of protective shells that make changes in the exchange protocols and data presentation formats to non-standard (unknown to the attacker), and having some potential for counteraction. The set of elements (tools) of protection is interpreted as the complexity of the information security system. Controversial assumptions have to be made about the unknown capabilities of the adversary, but the quality of the forecast in the field of intersubjective opposition should be distinguished from the prediction when countering the elements: the qualifications of the officials operating information technologies must be taken into account, and the fact that the actual course of the conflict is determined not only by the alignment (positional capabilities) of the forces and tools of the opposing parties. Information security system strategy is to distribute a limited non-uniform resource of protection tools to interdependent elements of the information infrastructure according to the strategy of the predicted impacts of the attacker. There is an antagonistic conflict with opposite goals (the so-called scheme of strict antagonism). We apply game theory and reduce this conflict situation to pair game with zero sum for the choice of the justified decisions [11-13]. The implementation of methods realizing power demonstrative blocking is passive, since it has no mechanisms to influence the enemy (passively expects information and technical impact), and in the case of high efficiency it can lead to frustration of the information needs of the enemy and force him to change the impact strategy and (or) compensate for the lack of information from other sources. The adversary can apply political, economic sanctions and other «levers» of pressure.

Let us proceed to the consideration of the third basic protective setting. It has a fundamental difference, namely, that it eliminates antagonism in the confrontation of the parties to the conflict. This is achieved by the fact that the application of the setting makes it possible to make the goals of the parties either independent or coincident. For example, when operating unlimited resources, conflict does not occur. For this purpose it is necessary that the information security system not only limits the variety of information technology (infrastructure) states, but also controls this diversity more constructively. In the case of exploitation of limited resources, but with the coincidence

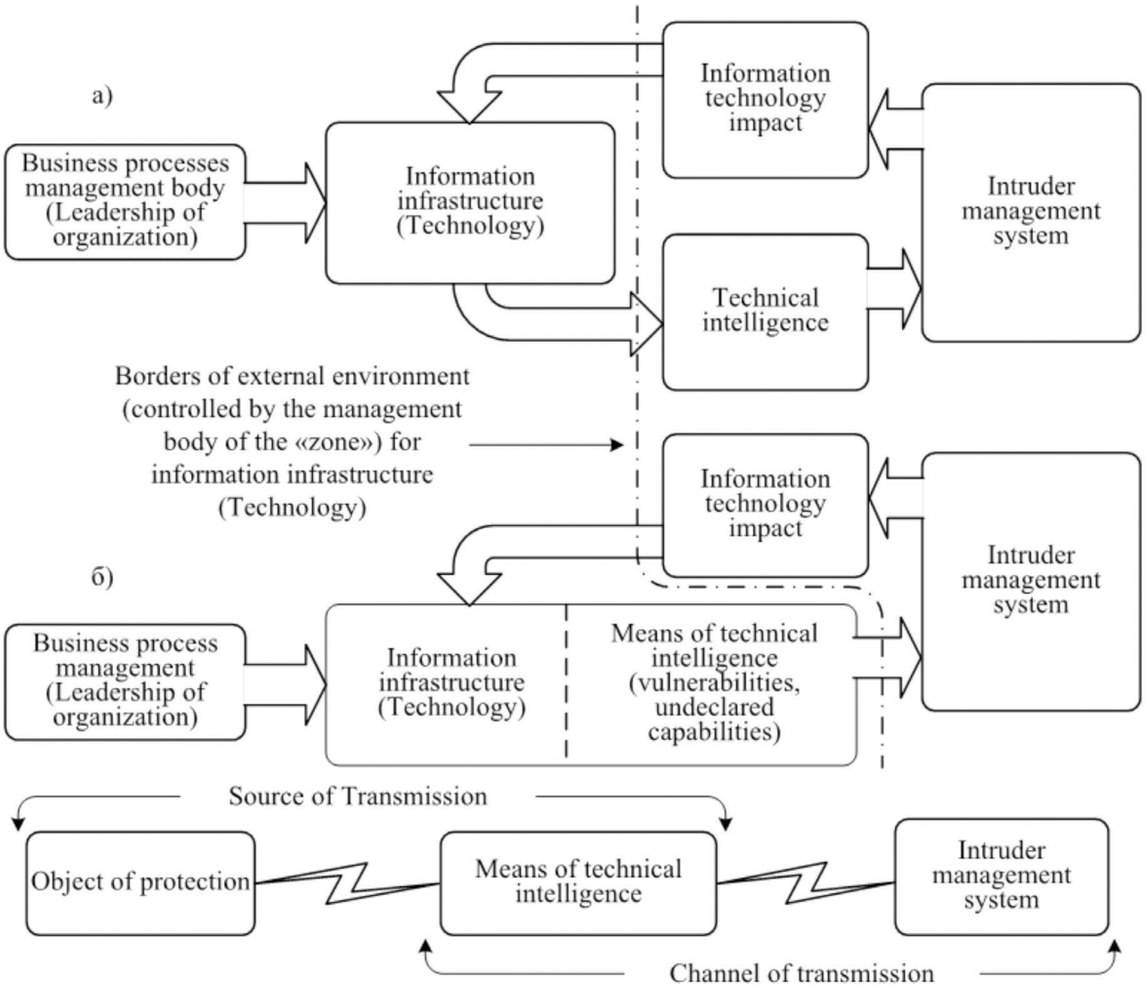

Fig. 6. Border of external environment for the allocated and cross-border information infrastructures and technologies

of interests, both parties are actually combined into one system. This happens if one assumes that the adversary makes a requirement of information content to the object of protection, and the means of obtaining information are present in the information infrastructure (technology). The boundaries of the external environment of the protected object (see Fig. 6) do not coincide with those adopted in the first and second protective settings (Fig. 6, a), and such an integrated system is the source of messages (Fig. 6, b) for the attacker's control system

(this always a subject) that forms wrong standards in his information space using the whole variety of information technology states [14]. However, instead of quantifying the informational messages received by the intruder's control system, it is possible to evaluate the benefit (non-profit) of the actions performed by the intruder on the basis of, as expected, the received and realized information.

Such actions (and the associated loss or gain for the object of protection) indirectly characterize the information on the basis of which these actions are performed. It turns out that there is no contradiction between the need to integrate and globalize information technologies and infrastructures, and the need to protect against the potential destructive capabilities of an opponent.

The ability to determine correctly the goals and capabilities of the opposing side, combined with the ability to find a compromise solution to the conflict, to comply with this compromise are rewarded by reducing the discomfort of the opponent [15, 16]. If the antagonism of the situation disappears, it is no longer reduced to pair game. A so-called «bimatrix game» arises, where each of the participants seeks to maximize his winnings, and not just to minimize the opponent's winnings. Existence of compromise solutions allows to anticipate perspective contradictions and, as a result, to predict a prize taking into account evolution of a subject to protection (change of information needs of officials). Analysis of the third protective setting suggests that the larger the object and the variety of its states, the easier it is to be protected, unlike traditional methods of protection (the first and second protective settings). Nevertheless, attempts to obtain results of a quantitative assessment of the share of innovations corresponding to the third setting show that this share is so negligible that it is not reflected in the information security reports of market leaders [17, 18].

The third setting implements the principle of non-conflict protection: efforts are not only transferred from the intense stages of the confrontation cycle, when the enemy is presented with distorted data aimed at his mistake, into less intense phases, but also allow to avoid conflict as a collision of protection tools and destructive information and technical impact, forming on the information space of the attacker a profitable «picture of the world» [19].

It is possible to implement such a principle (concept) when the variety of conditions that will be allowed by the regulations for ensuring information security will be no less than the potential diversity of information technology. This necessary condition follows from the Law of Requisite Variety formulated in, which can be simplified and applied to the subject area considered in the article as follows. The best use of information infrastructure and technologies for control purposes is possible if the diversity of the control system is not less than the diversity of the controlled system. However, at present, autocratic control of the information security system leads to the inevitable reduction of the diversity of the control system. The information security system cannot fully and comprehensively cover its information infrastructure and technologies with its regulations, and introduces a set of restrictions and prohibitions on elements beyond its control. In other words, in order to preserve the stability of management, the autocrat – the information security system – has to suppress a variety of information technologies. The inevitable result is a decrease in the effectiveness of innovation activities in the field of information technology, a defeat in competition with systems that encourage the growth of diversity.

Conclusions

A comparative analysis of the basic defensive settings implemented by information security systems and various types of protection tools leads to the following conclusions.

Firstly, the antagonistic games in no way affect with their descriptions conflicts with a number of parties greater than two. At the same time, there is a multilateral conflict in this subject area, which is fundamentally more complex than conflicts with two participants, and it does not even lend itself to the latter.

Secondly, even in conflicts with two participants, the interests of the parties are not at all obliged to be opposed. In many conflicts of this kind it happens that one of the situations is preferable to the other for both parties.

Thirdly, even if any two situations are compared by players in their preference in the opposite way, the difference in estimates of this preference leaves room for agreements, compromises and cooperation.

Finally, fourthly, the content sharpness of the conflict does not necessarily correspond to its formal antagonism. For example, if the traditional purpose of protection in countering intelligence – in response to intelligence seeking information, and the protection system seeks to hide it – can be changed to providing false, but reliable information on the attacker's criteria (as the third protective setting suggests) then the antagonism of a situation in its traditional understanding disappears.

Decision makers should understand that in the process of evolution of information technologies and infrastructure that irreversibly led to their globalization and transboundary nature, the confrontation has shifted to the third defensive setting [20], while information security systems basically have stopped at the second. The emergence of new and improvement of existing information technologies is constantly and almost continuously (for example, updates of Android applications come out in Google Play on average once every 28 days), while the processes of improving the information security system have pronounced functioning intervals with long regulated cycles [21]. The fair desire to verify the protection means with higher reliability is connected with the inability to significantly reduce these cycles and bring them closer to the rate of innovation in information technology. Ignoring

or insufficient understanding that the effective use of information technologies and innovative performance in the field of information technologies are undoubtedly constrained by the presence of autocratic control by the information security system, as existing and developing regulations will suppress technological diversity, will continue to lead to low rates of economic development and formation of information society from now on.

References

1. Information Security Threats during Crisis and Conflicts of the XXI Century / A.V.Zagorskii, N.P.Romashkina, eds. – Moscow, IMEMO RAN, 2016. – 133 p. DOI: 10.20542/978-5-9535-0461-4.
2. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96–99. DOI: 10.1109/CTSYS.2017.8109498.
3. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. - River Publishers, 2018. 458 p.
4. Mamzelev, I. A. i dr. Osnovy` sertifikacii i postroeniya oborudovaniya telekommunikacij / Pod red. I. A. Mamzeleva, L. V. Yurasovoj – M.: Radio i svyaz`, 2005. – 304 s. (in Rus).
5. Kastel`s, M. Galaktika Internet: Razmy`shleniya ob Internete, biznese i obshhestve / Per. s angl. A. Matveeva; Pod red. V. Xaritonova. – Ekaterinburg: U-Faktoriya (pri uchastii Gumanitarnogo un-ta). 2004. – 328 s. (in Rus).
6. A.V. Dorofeev, Y. V. Rautkin. Applied Aspects of Security Testing. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 49-53.
7. Barabanov A.V., Markov A.S., Tsirlov V.L. Methodological Framework for Analysis and Synthesis of a Set of Secure Software Development Controls, Journal of Theoretical and Applied Information Technology, 2016, vol. 88, No 1, pp. 77-88.
8. Reber, G., Malmquist, K., Shcherbakov, A. 2014. Mapping the Application Security Terrain. Voprosy kiberbezopasnosti [Cybersecurity issues]. 2014. N 1(2). P. 36-39. DOI: 10.21681/2311-3456-2014-2-36-39.
9. Shejnov, V. P. Skry`toe upravlenie chelovekom. M.: Izd-vo Xarvest, 2007. – 816 s. (In Rus).
10. Sokolovskij S.P., Orexov D.N. Konceptualizaciya problemy` proaktivnoj zashhity` integrirovanny`x informacionny`x sistem // Sbornik nauchny`x statej VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii «Nauchny`e chteniya imeni professora N.E. Zhukovskogo» 20-21 dekabrya 2017 goda / Ministerstvo oborony` Rossijskoj Federacii, KVVAUL im. Geroya Sovetskogo Soyuza A.K. Serova. – Krasnodar: Izdatel`skij Dom – Yug, 2018. S. 47-52. (In Rus).
11. Y. Wang, Y. Wang, J. Liu, Z. Huang, P. Xie. A Survey of Game Theoretic Methods for Cyber Security. In: 2016 IEEE First International Conference on Data Science in Cyberspace - DSC (Changsha, China, 13-16 June 2016), IEEE, 2016, pp. 631 – 636. DOI: 10.1109/DSC.2016.90.
12. R. Mitchell, B. Healy. A game theoretic model of computer network exploitation campaigns. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference – CCWC (Las Vegas, NV, USA, 8-10 Jan. 2018), IEEE, 2018, pp. 431–438. DOI: 10.1109/CCWC.2018.8301630.
13. R. Zhang, Q. Zhu. A game-theoretic analysis of label flipping attacks on distributed support vector machines. In: 2017 51st Annual Conference on Information Sciences and Systems - CISS (Baltimore, MD, USA, 22-24 March 2017). IEEE, 2017, pp. 1–6. DOI: 10.1109/CISS.2017.7926118.
14. Maximov R. V., Sokolovsky S. P., Gavrilov A. L. Hiding Computer Network Proactive Security Tools Unmasking Features. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 88-92.
15. Axelrod R., Iliev R. Timing of Cyber Conflict. In: Proceedings of the National Academy of Sciences of the United States of America, 111 (42014), January 28, 2014: 1298–1303.
16. Mulvenon J. Toward a Cyberconflict Studies Research Agenda. IEEE Security & Privacy. 2005, V.3, N 4, pp. 52-55.
17. Kozhevnikov D.A. Markovskaya model` upravleniya vzaimodejstviem sistem vedomstvennoj svyazi i programmno-apparatny`x vozdejstvij // Nauchno-texnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politexnicheskogo universiteta. Informatika. Telekommunikacii. Upravlenie. 2008. № 2 (55). S. 170-175. (In Rus).
18. Penyaz` A.L., Kolbasova G.S. Poisk novy`x texnicheskix reshenij po obespecheniyu strukturnoj skry`tnosti infokommunikacionny`x sistem special`nogo naznacheniya // Innovacionny`e texnologii: teoriya, instrumenty`, praktika. 2014. T. 2. S. 135-143. (In Rus).
19. Harris S. @War: The Rise of the Military-Internet Complex. - Eamon Dolan/Houghton Mifflin Harcourt, 2014. 288 p.
20. Davydov A.E., Maksimov R.V., Savickij O.K. Zashchita i bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh system -Moskva, 2015. – 520 s. (In Rus).
21. Markov A., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, pp. 213-231. DOI: 10.5772/intechopen.75232.