Conceptual model of the empirical data multidimensional presentation on the state of forming critical information infrastructure

A V Kalach¹², K O Burkova¹, T N Kulikova¹, E O Buharov³ and A N Scherbin¹
¹Voronezh institute of the Russian Federal Penitentiary Service, Irkutskaya 1a, Voronezh, Russia
²Voronezh State Technical University, Moskovsky pr-t 14, Voronezh, Russia
³Krasnodar Higher Military School, Krasina 4, Krasnodar, Russia

E-mail: AVKalach@gmail.com

Abstract. Conceptual model presented in the work is based on the synthesis of generalized representations comprising of the separate processes and phenomena which describe behavior of the investigated system (object) in the critical informational infrastructure. Conceptual model of providing cyber-resilience for the objects of critical informational infrastructure within the departmental information network integrated by informational-telecommunication public network into cyber-space and representing stochastic dynamics of the destructive informational impacts on the objects is given in the form of a common framework and processes (functioning, impacts and providing of cyber-resilience) which gives their most significant links.

1. Introduction
Various intrusions into security systems are inherent to the Russian area of the informational security in the different branches of economics and politics. Enterprises whose activity is related to the processing of payment information are traditionally considered as the leaders in the use of solutions providing information security.

Information on the state of the companies that do not process the payment data (for example, organizations that store data on the clients and their partners) do not necessarily mean informational security in this sphere.

As comparing with the whole world, Russia takes the leading place in the rating of information leakage, especially in such areas as the state authorities and law-and-order structures.

These area takes up to 39% of all the cases concerned with compromising of information registered in Russia (Table) [1–7]. The problem of data security comes first as in Russia, as in the world; they try to solve it due to the application of engineered safety features. Within the frameworks of solving complex problem for providing of cyber-security for the information system users the preliminary assessment of such systems is of a particular importance from the viewpoint of their security.

When assessing the state of security provision for cyber-resilient functioning in the conditions of destructive information impacts (DII) it is necessary to study critical informational infrastructure for the departmental information networks (CII DIN) as a complex active dynamic object. Providing the real parameters about the states of CII in the continuous dynamics and with the account of all the set of the effecting factors is a data flow.
Table Classification of the information leakage by the sources of information.

| Branch                          | World, % | Russia, % |
|--------------------------------|----------|-----------|
| Banks and financial institutions| 8.9      | 12.2      |
| Medicine                       | 19.0     | 8.5       |
| Commerce                       | 6.8      | 5.6       |
| High-Tech                      | 20.2     | 10.4      |
| Industry and transport         | 4.9      | 3.0       |
| State authorities and law-and-order structures | 13.9 | 23.3 |
| Education                      | 9.9      | 7.4       |
| Municipal institution          | 6.7      | 15.9      |
| Other/indeterminable           | 9.8      | 13.7      |

This data flow includes sets of the control signals and information representing rather heterogeneous and unmatched data characterizing the work of technical means for the information processing, software, services, commutation equipment and so on, comprising CII object [8–14].

2. Decomposition of the processes

A conceptual model for ensuring cyber stability of CII DIN objects integrated through a public information and telecommunication network into the state information system (IS) (SIS) and cyberspace representing stochastic dynamics of information impact (DII) on CII objects is understood as general schemes of CII objects studied in the theory of cyber-resilience, such as ACS DIN, information telecommunication space systems (ITSS), and the processes (functioning, impacts and ensuring cyber-resilience), thus presenting their most significant links (figure 1) [7, 15].

While accumulating statistical data large arrays of heterogeneous data are obtained related to the processes, phenomena, objects, subjects and so on, which are continuously replenished in the real-time mode (according to statistics, the ratio of the unstructured data to the structured ones equals three to two) [16, 17].

At present, there is rather great number of different approaches to the data analysis, from the routine ones using mathematical statistics methods up to those ones applying intellectual data processing techniques.

Each of these methods suggests a presentation of the collected data in a certain format in order to perform their further processing and obtaining of the results in the human-transparent form.

In order to apply the methods of mathematical statistics the information should be presented in the form of homogeneous data, while the intellectual data processing techniques make it possible to process rather heterogeneous and unmatched data [15, 17].

Analysis of experience in the application of intellectual data processing technologies [18] suggests that in order to present heterogeneous and unmatched information in the balanced form for its further analysis specially designed information data repositories are used for the data storage.

A distinctive feature of these data repositories is the ability to process the structured and unstructured information in common as a whole.
Figure 1. Conceptual model as a mean for the description of scientific knowledge about the objects of CII DIN.

The quality of the provided information after analytical processing with DSS system will be determined first of all by the amount of the accumulated empirical data and by the applied intellectual data analysis technique [15].

The necessity in accumulation of the empirical data in the specially designed information repository facilitates formation of the departmental electronic, continuously replenished archive of the behavioral activity of different objects starting from the technical facilities intended for processing information of the separate CII objects to CII DIN as a whole.

In order to do this it is proposed to build the corresponding multi-dimensional data base, figure 2.
Figure 2. Model of multi-dimensional presentation of the information on the state of CII objects.

Conclusions

Thus, utilization of the technology of the information repository along with the analytical processing of the information on the basis of multi-dimensional data base allows [15, 16]:

- to perform the most diverse and arbitrarily detailed classifications of one or another aggregate of external or internal, constructive and destructive informational impacts, actual output data and parameters describing the system and actions of the human component according to the most diverse signs. These classifications provide the most accurate understanding of interrelation between one or another characteristics of any CII objects thus ensuring analysis of as emergent as synergetic properties;
- to accomplish multidimensional statistical mathematical analysis. This analysis enables to find correlations between the most diverse parameters, characteristics events and so on. Theoretical models answer the question – why, and next, after detecting cause-and-effect principles make it possible to form recommendations on the order of procedure;
- to make prediction on the basis of classification and detected correlation of the factors, to determine the most reasonable way of the impact in order to gain that a set of the factors characterizing the current state of one or another CII object (parameters of the state, the official employing this state, different events and so on) would be transformed to the preset one for the required time that was predicted;
- to provide DSS with the required information to enable adequate control for the performance of CII DIN, accomplishing a full coverage of all the decided tasks including the problems of planning and forecasting which are usually difficult for automation.

References

[1] Data leakages. Russia. 2018 https://www.infowatch.ru/resources/analytics/reports
[2] Smirnov A I 2014 Global Security in the Digital Age: Stratagems for Russia (Moscow: All-Russian Research Institute of Geosystems) 394
[3] Makarenko S I 2016 Technical information weapons: terminology, classification, examples Control, communication and security systems 3 292-376
[4] Szeglov A Yu 2004 Protecting Computer Information from Unauthorized Access (SPB: Science and Technology) 384
[5] Lukatski A V 2001 Detection of the attacks (St. Petersburg.: BHV-St. Petersburg)
[6] Makarenko S I and Chuklyaev I I 2014 Terminology in the field of information confrontation Questions of cyber security 1(2) 13-21
[7] Zakharchenko R I, Korolev I D and Miroshnichenko E L 2017 Conflict in cyberspace: conceptual framework and terminology framework Works V of the International Scientific and Practical Conference
[8] Bazhenov L B 1978 Structure and functions of science theory (Moscow: Science) 225
[9] Radzhabov U A 1982 Dynamics of natural science knowledge (system-methodological analysis) (Moscow: Science) 336
[10] Zinovyev A A 1967 Foundations of logical theory of scientific knowledge (Moscow: Science) 261
[11] Pechenkin A A 1991 Substantiation of scientific theory (Moscow: Science) 184
[12] Greenyaev S N 2004 The battlefield is cyberspace. Information warfare theory, techniques, tools, methods and systems (Moscow: Harvest) 426
[13] Volkova V N and Emelyanova A A 2006 Systems Theory and System Analysis in Organization Management: Reference (Moscow: Finance and statistics) 848
[14] Volkova V N and Denisov A A 1977 Foundations of system theory and system analysis (SPb:Publishing House of SPbSTU) 512
[15] Barrels M V, Komarovich V F and Saenko I B 2002 Model of adaptive protection of information from in conditions of information confrontation Scientific and technical collection 4 21-5
[16] Simankov V C and Lutsenko E V 1999 Adaptive management of complex systems based on pattern recognition theory (Krasnodar: Publishing House of Kuban State University of Technology) 318
[17] Antonov V H, Terekhov V A and Tyukin I Yu 2001 Adaptive management in technical systems (SPb.: Publishing house of the St. Petersburg university) 244
[18] Sragovich V G 1976 Theory of adaptive systems (Moscow: Science) 319