UDK 519.257

PERSPECTIVES FOR THE USING OF BIG DATA TO ENSURE THE SECURITY OF CRITICAL INFORMATION SYSTEMS

I.N. Tsyrelchuk
Advisor to Rector, TUIT

D.S. Yakhshibaev
Dean of the Computer Engineering faculty of TUIT, PhD.

Kh.R.Jiyanbekov
Deputy Dean of the Computer Engineering faculty of TUIT

P.I. Soo
Professor of the Video Editing department of KUMA, South Korea

Yu. V. Pisetsky
Dean of the Joint faculty of Information Technology of TUIT, DtS.

Computer Engineering faculty of TUIT, Republic of Uzbekistan
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Republic of Uzbekistan
E-mail: hurshidj@gmail.com

I.N. Tsyrelchuk

Advisor to Rector, TUIT. PhD.

D.S. Yakhshibaev

He graduated from the National University of Uzbekistan. He is working as a Dean of the Computer Engineering faculty of TUIT. Also, he is an Associate Professor of the Department "Higher Mathematics". Conducts research on algorithms and models of integrated, applied mathematics.

Kh.R. Jiyanbekov

He graduated from the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi. He is a Deputy Dean of the Computer Engineering faculty, TUIT. In addition, he is an Associate Professor of the Department of "Information technologies" of TUIT. Conducts research on algorithms and models of big data analysis, data mining and cloud computing.

Yu. V. Pisetsky

Doctor of technical Sciences, associate Professor, Dean of the joint faculty of information technologies of the Tashkent University of information technologies and the Belarusian State University of Informatics and Radioelectronics

Park In Soo

He graduated from the Michigan State University. He is Professor of the Video Editing department of KUMA (Korean university of Media arts), South Korea.

Abstract. The Big Data plays a great role in the daily life of society. There are many types to ensure the security of systems. In this article were discussed new research method to ensure the security of critical information systems. Given new approach to support a defense to all kind of cyberattacks. In this article shown a simplified segment of the state graph of a modular-cluster network and its decomposition into core FLS subgraphs.

Keywords: big data, system, information system, critical information system, graph, subgraph, multigraph.

Introduction. There is a class of information systems, the safety of which is one of the basic requirements. These include, for example, systems for managing hazardous technological industries, transport, infrastructure management facilities, and others. Such information systems are called critical. The security of critical systems largely depends on the security of communication networks, which form the basis of the critical information infrastructure of a country or company that has a critical system. At different stages of the process of ensuring the security of a critical information infrastructure or information system, it is necessary to have a reliable assessment of the security of the information architecture.

The main stages of the information security process, the implementation of which requires an assessment:

- risk assessment of information security breaches;
- analysis of information flows and architecture;
- analysis of the threat model and information security violator;
- development of an information security policy;
- building an information security system;
- assessment of the effectiveness of the information security system;
- management of information protection processes and incidents;
- information security control.

To obtain a reliable assessment of the security of a complex information system, it is necessary to classify and analyze various physical and logical elements and the relationships between them, taking into account the dynamics of state changes, which involves the use of various modeling methods, as well as reducing the state graph to simplify the model in order to ensure the solvability of the problem.

However, any model is not accurate. With increasing complexity of the system, types and number of analyzed objects, the accuracy of the model decreases. For critical information systems, this situation is not acceptable, since there is a risk of information security incidents with significant damage.

The combination of modeling methods with Big Data technologies makes it possible to increase the reliability of the results of dynamic modeling of the states of complex information systems when solving problems of ensuring information security.

Consider the possibility of using Big Data technology to build an information system model and assess its compliance with security policy using the example of the modular-cluster network (ISS).

Materials and methods. In the ISS, the architecture of the critical information system is represented in the form of a FLS-multigraph, the vertices of which are physical and virtual (logical) modules, and arcs are the information relations between the modules. Typing of modules is based on the analysis of their cluster properties. Each module property is an interface that determines the module's ability to interact with other modules that have a similar (paired) interface. Interfaces are distributed according to hierarchical levels of information interaction: F-physical, L-syntactic and S-semantic. A set of FLS-interfaces of the module determines its ability to implement information primitives for information processing (transfer, storage, copying, modification, etc.).

The figure 1 shows a simplified segment of the state graph of a modular-cluster network and its decomposition into core FLS subgraphs. If the modules have the same type of interfaces at three levels, then the system switches to a new state, in which new modules are created or existing ones (graph vertices) and interfaces (graph arcs) are deleted. The presence of interaction levels of the modules allows you to simulate the dynamics of the information processing process, formalize the security policy and take into account the impact on the information process of information protection tools. For example, to take into account in the model the influence on the process of differentiating physical access to equipment, the differentiation at the level of syntactic access to information by cryptographic means, semantic access by means of delimiting the powers of users and programs. Modeling the state transition allows you to find all the possible trajectories of the information process.

Comparison of the declared security policy with all system states makes it possible to identify dangerous process paths in which unauthorized access to protection objects is possible. To ensure the practical applicability of the method to complex systems, the state graph is reduced by typing the modules and their interfaces, which deduces the analysis task from the class of NP-complete problems. This reduces the accuracy of the model and the reliability of the analysis results.

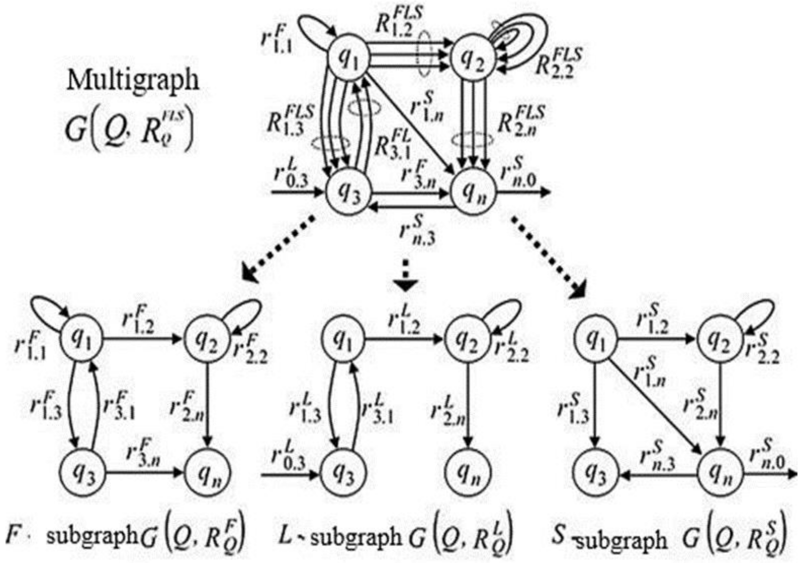

Figure *1.* – A simplified segment of the state graph of a modular-cluster network and its decomposition into core FLS subgraphs.

Effective solutions are often found in a combination of different methods. Some areas of application of Big Data technology for solving information security problems already have practical application, others are at the stage of development of a methodology for application or implementation.

The use of Big Data technology is a promising direction for improving the results of modeling and evaluating information security in combination with the methods of constructing and analyzing a modular-cluster network, which will increase the completeness of the information system model, the reliability and applicability of the analysis results due to:

– reducing the time to build a modular-cluster model of CIS (accelerating the identification and typing of modules and their interfaces);

– representations in the model of a larger number and types of elements and relationships, which are reduced under standard conditions;

– ensuring state monitoring, incident management and decision-making on information security online (speeding up state search procedures, identifying security event anomalies, ensuring the completeness of the knowledge base for forming decision options, etc.);

– visualization of the state graph of the system indicating the places of violation of security policy, etc.

Results. In addition to methodological, there are legal aspects of using Big Data to solve information security problems. In many applications, Big Data technologies are used to analyze personal data, including cross-border processing, which may be in conflict with national law.

In order to ensure legal legitimacy, it is advisable to develop and adopt the Big Data international information security standard, which defines the basic principles for their use, cross-border transfer, ensuring the rights of individuals and the application of protection measures.

Such an international standard can be adopted, for example, by the International Telecommunication Union, in which the 17th Security Committee operates.

The basic principles for ensuring the security of personal data when using Big Data technology in accordance with the Moorish resolution:

–Openness in information on the composition of the information collected its processing, the purposes of use and transfer to third parties.

–Determining the purpose of collecting information directly during its collection and limiting the use of data to an exclusively established purpose.

–Obtaining consent to the use of data.

–Collection and storage of only that amount of data that is necessary for the implementation of the intended legal goals.

–Providing personal access to individuals to the data that was collected about them, providing information about data sources and any algorithms used for the further development of their profile.

–Providing individuals with the opportunity to correct and manage their information.

–Analyzing how the collection of information affects the user's privacy.

–Anonymization (depersonalization) of data.

–Restriction and control of access to personal data.

Conducting a regular analysis to confirm that the profiling results are “reliable, fair and ethical, and also meet the purpose for which the profiles are used.”

Conclusion. The use of Big Data technology in order to solve the problems of ensuring information security in critical information systems, including by telecom operators, is a promising direction for increasing the level of information protection. In particular, the technology improves the reliability of information security assessments in critical applications.

It is advisable to standardize the issues of safe use of Big Data technology for use in the field of information security at the international level, to harmonize legislation under the new realities of the information society.

References

[1]. Informatica and Capgemini. The Big Data Payoff: Turning Big Data into Business Value, 2016.

[2]. V. Kayser, B. Nehrke, D. Zubovic. Data Science as an Innovation Challenge: From Big Data to Vlaue Proposition, Technology Innovation Management Review, 2018.

[3]. M.S. Hopkins, R. Shockley. Big Data, Analytics and the Path from Insights to Value, MITSloan Management Review, 2011.

[4]. Harvard Business Review. The Enterprise Lacks a Big Data Strategy for IoT Transformation, 2017, pp.1-12.

[5]. S. Lavalle, M.S. Hopkins, E.Lesser, R. Schockley, N. Krushcwitz. Analytics: The New Path to Value, MITSloan Management Rev., 2010.

[6]. S. Viaene, A. Van den Bunder. The secrets to managing business analytics projects, MITSloan Manag. Rev., 2011, pp. 65–69.

[7]. A. Chebotko, A. Kashlev, S. Lu. A Big Data Modeling Methodology for Apache Cassandra. Proc. of IEEE Int. Congress on Big Data, 2015, pp.238- p.245.

[8]. A. Fink, R. Guzzo. S. Roberts. Big Data at Work: Lessons from the Field, Society for Industrial and Oranizational Pshchology, 2017.

[9]. S. Nalchigar, E. Yu. Business-driven data analytics: a conceptual modeling framework, Data & Knowledge Engineering, 2018, pp. 1-14.

[10]. M.A. Berry, G.S. Linoff. Mastering data mining: the art and science of customer relationship management, Industrial management data system, 2000.

PERSPECTIVES FOR THE USING OF BIG DATA TO ENSURE THE SECURITY OF CRITICAL INFORMATION SYSTEMS

I.N. Tsyrelchuk
Advisor to Rector, TUIT

D.S. Yakhshibaev
Dean of the Computer Engineering faculty of TUIT, PhD.

Kh.R. Jiyanbekov
Deputy Dean of the Computer Engineering faculty of TUIT

Park In Soo
Professor of the Video Editing department of KUMA, South Korea

Yu. V. Pisetsky
Dean of the Joint faculty of Information Technology of TUIT, DtS.

Computer Engineering faculty of TUIT, Republic of Uzbekistan
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Republic of Uzbekistan
E-mail: hurshidj@gmail.com

Abstract. The Big Data plays a great role in the daily life of society. There are many types to ensure the security of systems. In this article were discussed new research method to ensure the security of critical information systems. Given new approach to support a defense to all kind of cyberattacks. In this article shown a simplified segment of the state graph of a modular-cluster network and its decomposition into core FLS subgraphs.

Keywords: big data, system, information system, critical information system, graph, subgraph, multigraph.