RESEARCH OF INFORMATION PROTECTION METHODS IN COMPUTER SYSTEMS FOR MONITORING AND DIAGNOSTICS OF ELECTRIC SUPPLY OF RAILWAYS

Halyna Holub
PhD, Associate Professor
Department of Automation and Computer-Integrated Technologies of Transport[1]
golub.galina@ukr.net

Olena Soloviova
PhD
Department of Theoretical and Applied Mechanics[1]
ealena_konoplya@bigmir.net

[1]*State University of Infrastructure and Technologies*
9 Kyrylivska str., Kyiv, Ukraine, 04071

Abstract: In modern conditions of growth of informatization, to ensure the reliability of the functioning of distributed computer information-diagnostic and control systems, which are mandatory for consideration, there are problems of assessing security and implementing protection of operational information.

The state of information protection and the reliability of computer systems for corporate monitoring and diagnosis of the railway power supply system are analyzed. The main tasks in the intellectualization of component systems are defined, namely traction electric network. The principles of information protection are proposed, which include: active protection of information; convincing protection of information, consisting in the justification of the design and measures to protect the conditions and circumstances. Such a principle as the continuity of the information protection process provides for the organization of the protection of objects at all stages of the development and operation life cycle. A variety of information protection tools provides for the exclusion of patterns at the stage of selecting cover objects and various ways to implement protection, not excluding the use of standard solutions.

The combination of the above principles in the work is called an integrated approach to information security, which is the basis for the creation of computer information protection systems. According to the sphere of information security, this approach complies with international ISO standards, and for the technical protection of information and state standards it complies with the requirements of existing national legislative and regulatory documents.

To ensure the security of information stored and processed in computer systems, the coordinated application of various security measures is necessary.

Keywords: information protection, computerization, principles, information security, technological process, computer systems.

1. Introduction

The distributed traction power supply network of the railway transport is part of the unified energy system of Ukraine, but at the same time, it has a number of features. These include a large non-uniformity of "moving" loads, a significant asymmetry of the supply voltage and non-sinusoidality, since the power supply procedure is implemented between phases $u_a(t)-u_c(t)$ or $u_b(t)-u_c(t)$. The features of the system also include the difficulties of protection against short circuit, a high level of physical and moral deterioration of electrical equipment. These features significantly contribute to a significant increase in energy consumption and the development of systemic accidents that lead to multimillion-dollar economic losses. The solution to the complex problem of optimizing energy supply, energy conservation and reliability and quality of transportation is possible based on the organization of modern intelligent network technologies as the basis for the innovative transformation of traction electric networks of railways.

When intellectualizing the traction electric network, much attention is paid to the tasks of intellectual processing of primary information to optimize the processes of energy management. Thanks to this, on the basis of promising information and network technologies, the opportunity will open up for the development and use of computer intellectualization methods for operating modes of railway traction networks. At the present stage, this is possible by presenting primary information in the required form, as well as by forming options for possible operational solutions to dispatch personnel [1, 2]. As practical experience [3, 4] shows, protection in modern conditions requires almost any information that is valuable to its owner in terms of its misuse by unauthorized users. That is why, the application of measures and means of computer systems and information security networks has become mandatory for any computer systems and networks.

2. Methods

It is planned to carry out a complex of organizational changes, build new process models, attract new solutions in the field of information technology, new ways and means of informatization, as well as intellectualize the control processes of traction electric networks of railways [5]. And the implementation of monitoring and forecasting reliability, increasing work efficiency, optimizing power consumption, improving traffic safety and innovating in the creation of information protection methods in computer systems for monitoring and diagnosing electric power systems.

3. Results

The management of the electric power industry at the present stage is characterized by a large increase in the volume of information that is formed during computer monitoring and control of the parameters of technological processes in electric power facilities and networks for the formation of managerial decisions [6]. At the same time, mathematical models and methods for controlling the modes of power consumption in rail transport from system-wide positions are not sufficiently developed. In existing methods for predicting electrical loads, there are stringent conditions for the primary information received, the behavior of electric power control objects, and therefore, they can't always satisfy the modeling accuracy for operational control. In order to prevent accidents and reduce losses, change the characteristics and scheme of the network, the main problem is information on the reliability of networks [7].

Computer systems for corporate monitoring and diagnosing the state of electric power facilities and systems allow early detection of threats to damage to main equipment and prevent emergencies that may develop in an accident.

To ensure continuous monitoring of the parameters of the regimes of electric networks of the railway, the principle of synchronism and unity of measurement of primary information is used as the basis for choosing operational management procedures and ensuring the functioning of distributed databases. The core of informatization of the operational dispatch control process is an integrated primary data environment, formed from a single system-wide information position, in conjunction with data processing methods.

Primary information reflects the parameters of the system modes, the state of electrical equipment is subject to intellectual processing in order to generate diagnostic conclusions and control actions at the level of power supply distances or the power supply system as a whole [8]. Primary information is archived, and in accordance with regulatory documents, is stored in raw form. In addition, the problem of computerization of technological processes at the substation level is also associated with the organization of commercial electricity metering, which includes metering of distribution, consumption, transportation, and electricity generation.

A set of tasks related to the registration and formation of an integrated environment of primary information, for the organization of control actions and its transfer for further use at the following levels of management, is solved automatically. This is due to the computerization of lower-level fast processes.

Since the monitoring process can accumulate large amounts of primary information, the server must be protected by a complex of hardware-software tools or an information security system from unauthorized access. And for the timely transmission of information to higher levels of management, the local network server must work through a remote office router that connects the local network to a regional or central corporate network.

Wide area monitoring systems (WAMS) are gradually being included in the structure of automated control of energy systems. As a result, the full realization of the potential of the WAMS infrastructure requires the solution of priority issues of information security and reliability.

In order to minimize the consequences of unauthorized access to information by unauthorized users, the leading role is given to increasing the efficiency of existing and promising integrated information protection systems [9, 10]. Although an information security system will be more effective, it is being developed in conjunction with a computer system where security tools can be used. Namely, both existing ones and developing special ones for a particular system depending on its features, operating conditions and requirements. To effectively protect information, when building these systems, a preliminary analysis of possible threats to the security of the computer system that is being protected is performed.

When organizing effective and reliable information protection in computer systems and networks, relying on requirements for protecting information from unauthorized access, they are guided precisely by organizational principles. It is such protection, taking into account all the requirements for information protection that is called an integrated approach to ensuring information security, which is the basis for creating a promising integrated system for ensuring information security (**Fig. 1**).

The study of methods and models of processes of attack on information, which allow assessing the level of security of computer systems from unauthorized access methods, is the basis for the creation of computer information protection systems.

Now the vast majority of information security vulnerabilities in corporate computer systems for monitoring and diagnostics are inherent in components and technologies of the upper levels of the hierarchy. To the lower levels, which are represented by registration devices, reliability is determined by the ability of PMUs to provide full functionality according to the specification and their level of maintainability. According to the structure of the corporate system for monitoring and diagnosing transients of the power supply system, one of the key objects for reliability is the main server of the power supply distance information network. Its functions are to form a single information space of primary information received from PMUs of traction substations of a distance of power supply, implement information exchange procedures with a central corporate network, and maintain a database of primary emergency and commercial information. Such multitasking of the main server determines the complexity of the information security systems used and the need to use updated information security models to assess the level of security of a given network element [11].

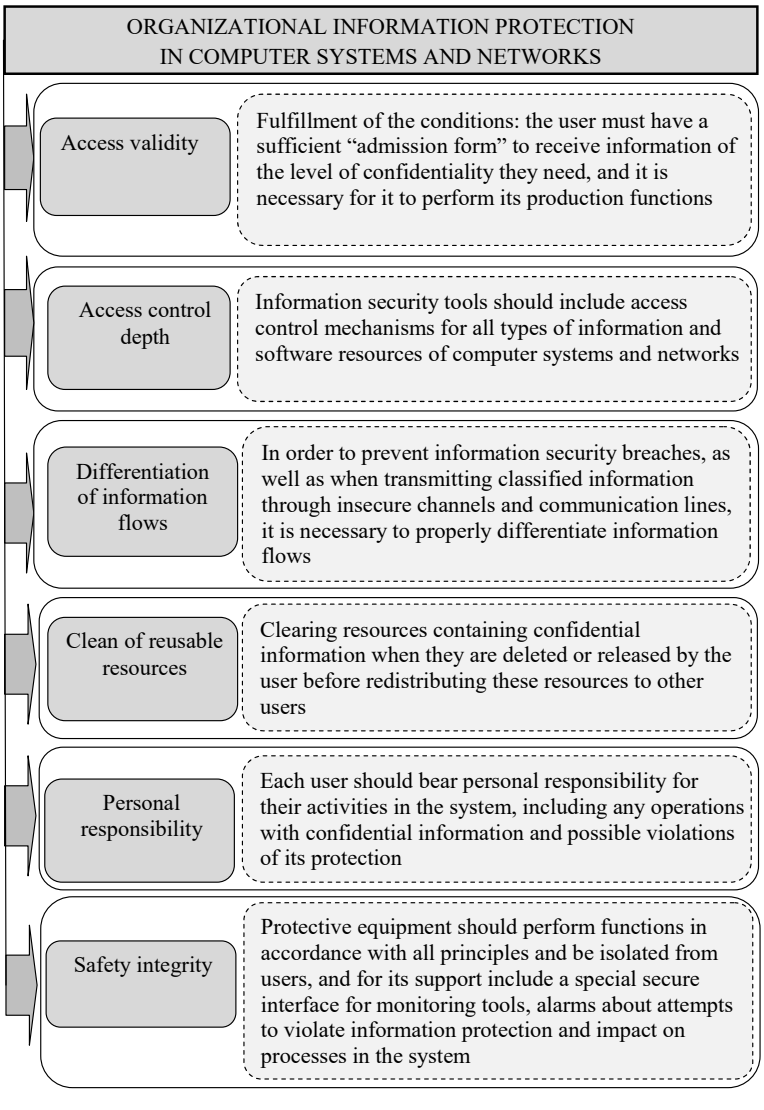

Fig. 1. The principles of an integrated approach to information security

The server in the system at the current time is in one of the typical states S, under the influence of information protection methods changes states, with corresponding probabilities, for some time T [11]. At the same time, a mathematical model of information security for assessing the level of security of network elements with the probabilities of states S_0 and F_0:

$$\begin{cases} P_{S0}(t) = \prod_{i=1}^{n} P_{Si}(t), \\ P_{F0}(t) = 1 - \prod_{i=1}^{n} \left(1 - P_{Fi}(t)\right), \end{cases} \quad (1)$$

where S_0 – server uptime, which provides for full functionality, that is, the simultaneous stay of the system in the $S_1 ... S_n$ states, which can be considered independent events; F_0 – server failure in any of the functionalities is an event that occurs when at least one of the independent failures $F_1 ... F_n$ occurs.

Thus, information processing of operational information, distributed more to the lower levels of the hierarchy, will improve the reliability and efficiency of the railway transport power supply system when implementing information security systems.

4. Discussions and conclusions

The analysis of the main vulnerabilities of distributed computer systems for monitoring and diagnostics of electric power systems is carried out. The basic requirements of information security are established, which should be provided in modern conditions, when operating diagnostic systems, consisting in the implementation of information security systems at the upper hierarchical levels of corporate computer systems. From the point of view of information security, the main prerequisites for the introduction of full-fledged automated control of the power system modes have been established, which are the widespread introduction of information security systems at all levels of corporate systems, the implementation of diagnostic procedures and redundancy.

References

1. Golub, G. M. (2017). Reliability control of failure-free operation of power supply system of railroad and its components by methods of intellectualization and informatization. Metallurgical and Mining Industry, 5, 8–13.
2. Kulbovskyy, I. I., Golub, G. M. (2016). Analysis of normative and technical base of the introduction of Intelligent energy systems based on SMART GRID technology. Informatsiyno-keruiuchi systemy na zaliznychnomu transporti, 3, 50–57.
3. Lenkov, S. V., Peregudov, D. A., Horoshko, V. A. (2008). Metody i sredstva zashchity informatsii. Vol. 2: Informatsionnaya bezopasnost'. Kyiv: Ariy, 344.
4. Stasyuk, A. I., Goncharova, L. L. (2017). Mathematical Models and Methods of the Analysis of Computer Networks of Control of Power Supply of Railways Traction Substations. Journal of Automation and Information Sciences, 49 (2), 50–60. doi: https://doi.org/10.1615/jautomatinfscien.v49.i2.50
5. Stasiuk, O. I., Grishchuk, R. V., Goncharova, L. L. (2018). Mathematical Differential Models and Methods for Assessing the Cybersecurity of Intelligent Computer Networks for Control of Technological Processes of Railway Power Supply. Cybernetics and Systems Analysis, 54 (4), 671–677. doi: https://doi.org/10.1007/s10559-018-0068-2
6. Stasiuk, A. I., Goncharova, L. L., Maksymchuk, V. F. (2014). Methods of intelligent railway electrical power systems organization based on SMART Grid concept. Informatsiyno-keruiuchi systemy na zaliznychnomu transporti, 2, 29–37.
7. Kulbovskyi, I. I., Holub, H. M., Haydenko, O. S. (2018). Modeling of information powers of computer monitoring of the network of electrical supply of transport. Metallurgicheskaya i gornorudnaya promyshlennost, 4, 94–98. doi: https://doi.org/10.33101/s04-4757684
8. Butkevych, O. F., Levkonyuk, A. V., Stasiuk, O. I. (2014). Increasing reliability of monitoring of acceptability of loading of power system's controlled cutsets. Tehnicheskaya elektrodinamika, 2, 56–66.
9. Kalyniuk, I. O. (2011). Metody udoskonalenoho upravlinnia protsesamy peredachi v kompiuternykh merezhakh. Informatsiyno-keruiuchi systemy na zaliznychnomu transporti, 5, 43–46.
10. Voronko, I. O. (2013). Zakhyst informatsiyi v kompiuternykh systemakh i merezhakh na osnovi teoriyi ihor. Avtomatyzatsiya ta kompiuterno-intehrovani tekhnolohiyi u vyrobnytstvi ta osviti: stan, dosiahnennia, perspektyvy rozvytku: mat. vseukr. nauk.-prakt. internet-konf. Cherkasy, 54–57.
11. Stasiuk, A. I., Goncharova, L. L., Golub, G. M. (2017). Method for Assessing Cybersecurity of Distributed Computer Networks for Control of Electricity Consumption of Power Supply Distances. Journal of Automation and Information Sciences, 49 (7), 48–57. doi: https://doi.org/10.1615/jautomatinfscien.v49.i7.40

Received date 02.10.2019
Accepted date 29.10.2019
Published date 23.11.2019