SOFTWARE FOR EVALUATING THE ELECTRONIC SAFETY SYSTEM RELIABILITY IN CASE OF LARGE VOLUME OF DATA ABOUT ITS TECHNICAL CONDITIONS AVAILABILITY

S.S. DZIK
Master of Information and Computer Systems BSUIR

N.I. TSYRELCHUK
Master of Information and Computer Systems Design BSUIR

S. BOROVIKOV, PhD
Associate Professor, Department of Information and Computer Systems Design BSUIR

I. TSYRELCHUK, PhD
BSUIR Lifelong and E-learning Studies Faculty Dean, Information and Computer-aided Systems Design Department Head, PhD, associate professor

S.K. DZIK, PhD
First BSUIR vice-rector, PhD, associate professor

N. ZHIDILIAEVA
Foreign Languages Department №1 teacher, BSUIR

The Belarusian State University of Informatics and Radioelectronics, Republic of Belarus
E-mail: sdick@bsuir.by, tsyrelchuk@bsuir.by, bsm@bsuir.by, nzhidilyaeva@gmail.com

Abstract. Evaluation of the design reliability of a complex electronic system causes many difficulties. This is a consequence of an excessive number of possible technical states of the system. In a number of cases, the number of these states and the data volumes for their description is so large that they fall under the notion of Big data. As the result, the usual methods of processing such volumes of data are not possible. As a way out of the situation, we propose to use the simplification of analysis which is based on the decomposition of the system.

We have developed software for applying the decomposition method to assess the reliability of electronic security systems. It allows you to build a protected object (the building plan with its premises) in an interactive mode with the help of a computer, place the components of an electronic security system in the premises, allocate subsystems and perform their analysis in terms of the reliability and protection of the premises.

The reliability of a technical system is one of its most important properties. This property largely determines the success of the task assigned to the system. Therefore, when designing a technical system of any functional purpose, the question of predicting the index of its reliability is urgent [1]. Such indicator should be considered as the efficiency preservation coefficient C_{ep} or its modifications [2]. Coefficient C_{ep} in accordance with State Standard 27.002-89 is a generalized name of a group of indicators used in various industries and having their own names, designations and definitions [3]. For electronic security systems, it is appropriate to consider the probability of ensuring the security of an object or an individual as such an indicator. The value of this indicator depends on both the reliability of the technical devices included in the system, and the probabilities of perception and/or the correct threat signals processing. The values of these probabilities are determined by the temporary failures of the system's devices, which are the consequence of the external environment influence (climatic factors, electromagnetic influences, etc.) on the system and its constituent parts [4, 5].

To quantify the probability with which the security of an object is ensured, it is necessary to consider the possible technical states of the system and to take into account the efficiency coefficients corresponding to these states. It is logical to use the probabilities of object protection as the efficiency coefficients (provided that the system is in this technical condition). Technical conditions of the system are determined by the technical states of the devices included in it [6]. For devices, as a rule, one of two states can exist: either inoperative or operable, while for the system as a whole there are many states that differ by combinations of operability and inoperability of system devices. Some of these states correspond to the state of inoperability of the system as a whole, others - to the state of operability. Depending on the combination of technical states (operable or inoperative), the functioning state of the electronic security system is characterized by different probabilities of object protection, or, it is said, different functioning efficiency.

Estimation of functioning efficiency of a complex electronic security system by considering the system as a whole in practice causes many difficulties due to the excessive number of possible technical states of the system S, which is defined as

$$S = 2^{n}, \tag{1}$$

where *n* is the total number of technical devices included in the electronic security system.

For example, in the case when a building contains 30 rooms and the installation of only one sensor on each entrance door and on each window (with one window in the room) is available, the number of possible technical states of the electronic security system will be

$$S = 2^{30+30} \approx 1{,}153 \cdot 10^{18}.$$

Which is important, this number takes into account only the sensors but not other devices of the electronic security system.

Considering that dozens of memory bytes are needed to store data on one technical state of the system, the total amount of data necessary to describe all possible technical states of the electronic security system can amount to a number that falls under the concept of Big Data [7].

Thus, the effectiveness of the electronic security system analysis is associated with the examination of a large amount of data about the system state. In this case it is impossible to process such a volume of data by traditional methods. The question arises, what is the way out of this situation, how to take into account the large amount of data on possible technical conditions of the electronic security system?

To solve the problem for engineering practice various methods for simplifying the analysis of system reliability can be proposed. One of these methods is decomposition [5, 8]. Its essence consists in dividing the system under consideration into smaller subsystems, each of which is much easier to analyze than the original system. Upon receiving reliability indicators of the subsystems it is relatively easy to find the reliability index of the system as a whole.

For analyzing the reliability of the electronic security system by the decomposition method application software was developed at the Information and Computer Systems Design Department of BSUIR. Below are the explanations that allow you to get the most general idea of this software.

The developed software allows to create a plan of the building in an interactive mode, to place sensors, video cameras and other security devices on the building premises, to allocate subsystems in the initial system on the basis of the composition and interaction of the technical devices of the system consideration, i.e., in fact, perform the decomposition of the system, analyze the effectiveness of the of premises protection using the allocated subsystems, determine the efficiency (reliability) of the system as a whole. The probability of the premises protection (with the help of the electronic security system) from an offender’s penetration is considered as an indicator of the effectiveness of the functioning of the system.

Figure 1 depicts the main window of the developed software. The menu bar at the top of the window is used to select the user's actions during preparation (configuration) and project execution. You can choose to execute a new project and save the results of its development and calculation, or open a previously saved project and continue its execution.

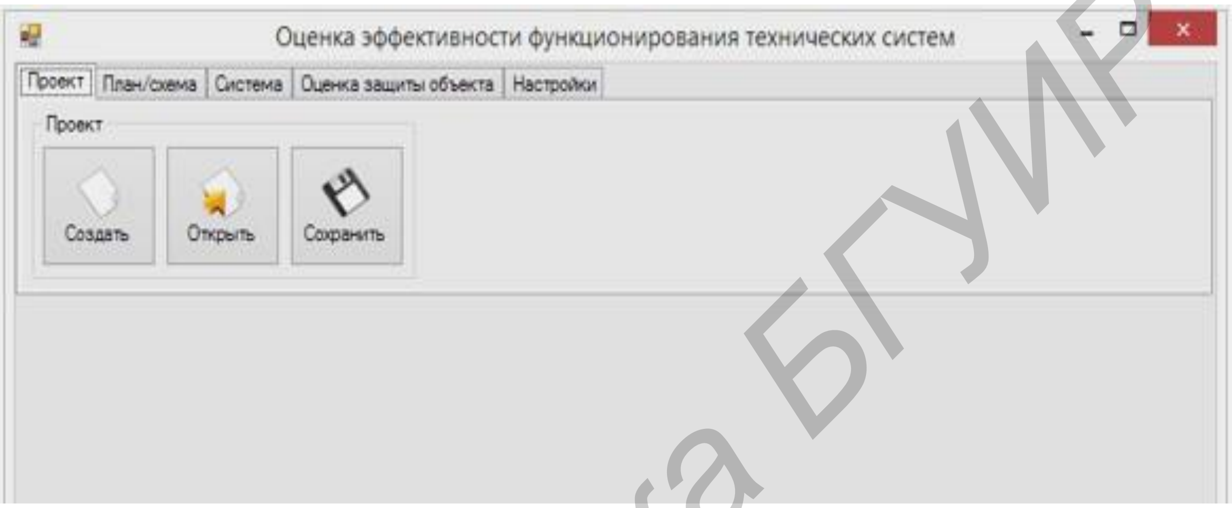


Fig. 1. Main window of the software tool

Figure 2 demonstrates a fragment of a constructed building plan, the premises of which will be protected by an electronic security system.

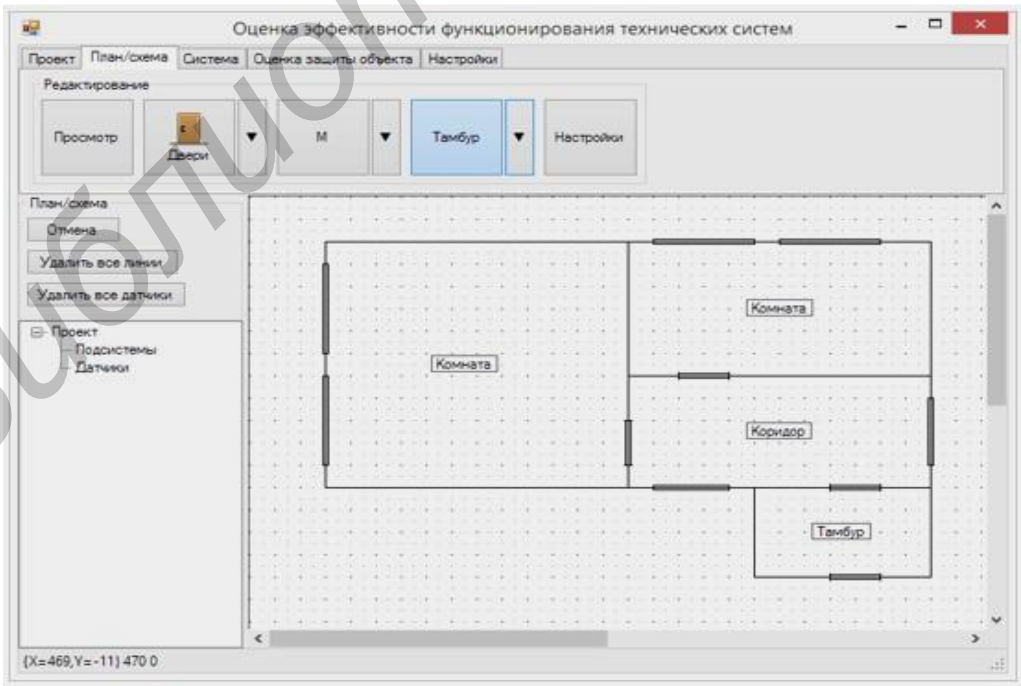
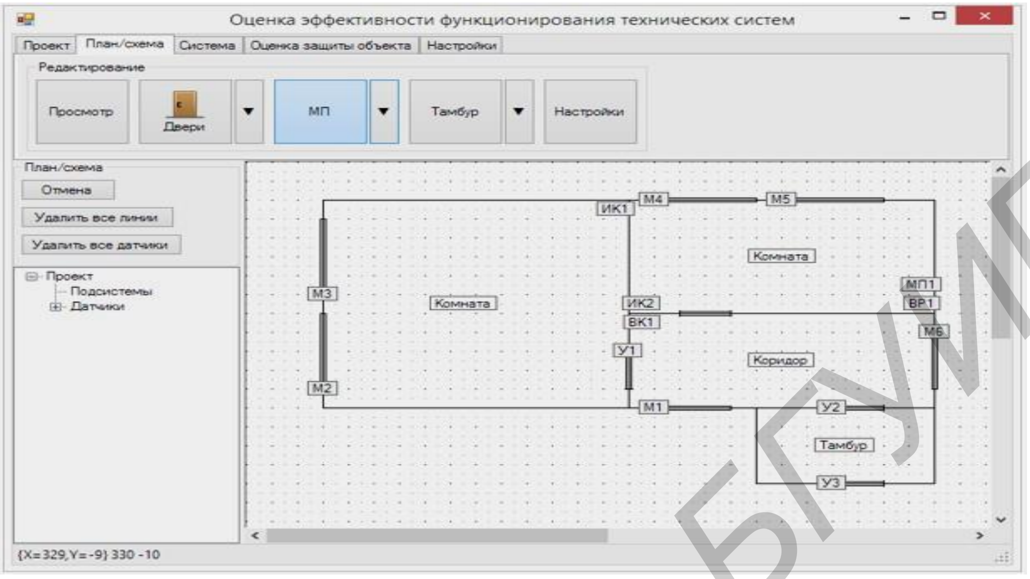


Fig. 2. Fragment of the protected building premises plan

The plan of the object (building premises, see Figure 2) is designed by a user with the help of the graphical capabilities of the software and the tools provided for editing the plan.

Figure 3 illustrates one of the options for the user to place sensors and other devices of the electronic security system on the built-up plan of the building's premises.

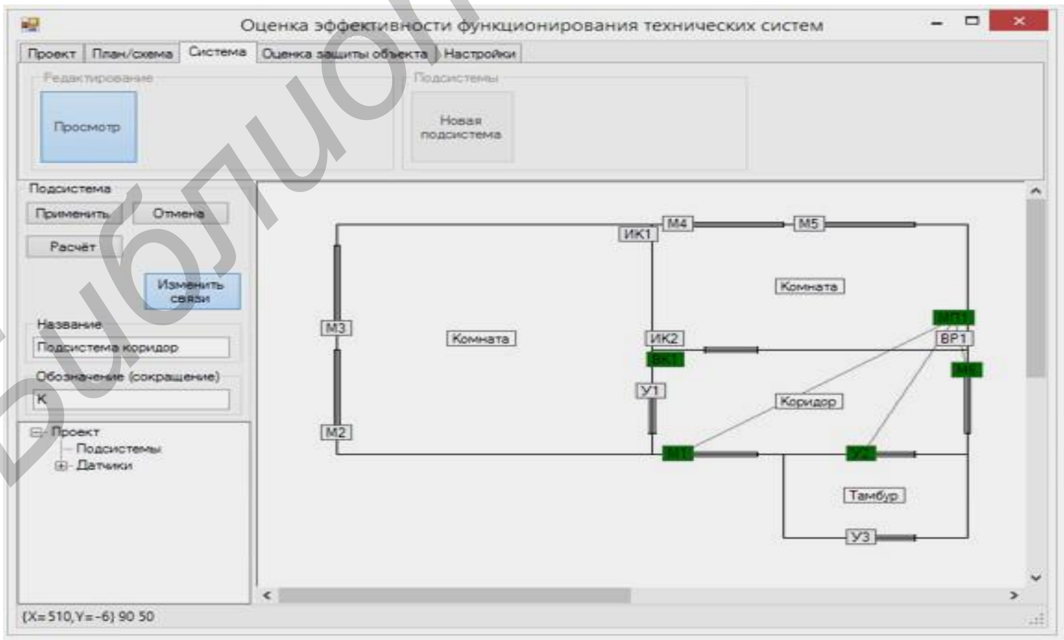


{X=329,Y=-9} 330 -10

Fig. 3. Example of placement of system devices in the premises of a building

In Figure 3 the following designations are used: М1 ... М6 - magnetic contact sensors; У1 ... У3 - shock sensors; ИК1, ИК2 - infrared motion sensors; ВК1 - video camera; ВР - DVR; МП1 - microprocessor receiving and monitoring device.

Figure 4 illustrates the allocation of the subsystem, i.e., the actual implementation of the electronic security system decomposition.



Название: Подсистема коридор

Обозначение (сокращение): К

{X=510,Y=-6} 90 50

Fig. 4. Selection of the subsystem from the system devices

Let us describe the basic principles of decomposition with reference to electronic security systems. On the one hand, the subsystems should be distinguished from the condition of counteracting the infiltration of the intruder into the building's premises; on the other hand, they should be simple. The number of devices in the subsystems should not exceed 4 ... 6 units. The same subsystem device can be a part of two or more subsystems, for example, the МП1 device will be a part of all subsystems that will include at least one sensor, since the threat signals generated by the sensors arrive for processing at the device МП1 - microprocessor- control device. When real projects are implemented, the number of allocated subsystems having the same composition of devices and their interaction may turn out to be a remarkable number: dozens, sometimes hundreds.

The electronic security system functioning efficiency indicator (in the form of the probability of the object protection Pprot) is relatively simple to be obtained from the results of the subsystems performance analysis.

Thus, the use of complex technical systems decomposition makes it possible to isolate homogeneous information (to do system decomposition) from a large amount of data (Big Data) about possible technical states of a complex system and keep completing the task by traditional methods.

References

[1]. Borovikov, S. Prediction in Big Data Technology / S. Borovikov, E. Shneiderov, N. I. Tsyrelchuk, S.S Dzik // BIG DATA and Advanced Analytics. Использование BIG DATA для оптимизации бизнеса и информационных технологий : сб. материалов II Междунар. науч.-практ. конф. (Минск, Республика Беларусь, 15–17 июня 2016 года) / редкол. : М.П. Батура [и др.]. – Минск : БГУИР, 2016. – С. 98–101.

[2]. Надёжность в технике. Основные понятия, термины и определения. ГОСТ 27.002–89. – М. : Изд-во стандартов, 1990.

[3]. Состав и общие правила задания требований по надёжности. ГОСТ 27.003-90. – М.: Изд–во стандартов, 1991.

[4]. Боровиков, С. М. Теоретические основы конструирования, технологии и надёжности : учебник для инж.-техн. спец. вузов / С. М. Боровиков. – Минск : Дизайн ПРО, 1998. – 336 с.

[5]. Надёжность технических систем : справочник / Ю. К. Беляев [и др.] ; под ред. И. А. Ушакова. – М. : Радио и связь, 1985. – 608 с.

[6]. Цырельчук, Н.И. Оценка надёжности электронной системы методом анализа множества её технических состояний / Н.И. Цырельчук, С. М. Боровиков, С. С. Дик, И. Н. Цырельчук // Современные средства связи: материалы XXI Междунар. науч.-техн. конф., 20–21 окт. 2016 года, Минск, Респ. Беларусь; редкол.: А.О. Зеневич [и др.]. – Минск: УО ВГКС, 2015. – С. 126–127.

[7]. Batura, M. Big Data Volumes and Some Approaches to the Creation of Corporate Analytical Systems / M. Batura, S. Dzik, I. Tsyrelchuk, S. Borovikov // BIG DATA and Advanced Analytics. Использование BIG DATA для оптимизации бизнеса и информационных технологий: сб. материалов II Междунар. науч.-практ. конф. (Минск, Республика Беларусь, 15–17 июня 2016 года) / редкол. : М.П. Батура [и др.]. – Минск : БГУИР, 2016. – С. 74–80.

[8]. Дик, С.С. Прогнозирование эффективности функционирования электронной системы при наличии большого объёма данных о её технических состояниях / С.С. Дик, С. М. Боровиков, Н. И. Цырельчук, С.К. Дик // Современные средства связи: материалы XXI Междунар. науч.-техн. конф., 20–21 окт. 2016 года, Минск, Респ. Беларусь; редкол.: А.О. Зеневич [и др.]. – Минск: УО ВГКС, 2015. – С. 377–378.