Simulation modelling as a tool to diagnose the complex networks of security systems

S Y Iskhakov\textsuperscript{1}, A A Shelupanov\textsuperscript{1}, R V Meshcheryakov\textsuperscript{1}

\textsuperscript{1} Tomsk State University of Control Systems and Radioelectronics, 40, Lenina ave., Tomsk, 634050, Russia

E-mail: frosty86@mail.ru

Abstract. In the article, the questions of modelling of complex security system networks are considered. The simulation model of operation of similar complexes and approbation of the offered approach to identification of the incidents are presented. The approach is based on detection of uncharacteristic alterations of the network operation mode. The results of the experiment allow one to draw a conclusion on possibility of the offered model application to analyse the current status of heterogeneous security systems. Also, it is confirmed that the application of short-term forecasting methods for the analysis of monitoring system data allows one to automate the process of formation the criteria to reveal the incidents.

1. Introduction

The prompt development of security system market over the last years is caused by the increase of topicality of international terrorism threat, anthropogenic and natural disasters and, also, the growth of cyber-crime and industrial espionage. In practice, the problem of development of a uniform security system complex often arises. A widespread approach to its solution is the integration of heterogeneous equipment on the basis of local area networks (LAN). The main units of the involved systems connect in the complex security system network (CNSS).

The CNSS is a heterogeneous complex of software and hardware which differs in principles of operation and types of the provided information, but performs a common task - to provide security of people’s lives and health and to decrease the probability of material damage to a company.

The development of a security system sector is impossible without implementation of science intensive technological solutions. Scientists all over the world work on the development of new ways to detect threats, to simulate the behaviour of operations of malefactors etc. The majority of modern research is directed to the solution of theoretical and practical tasks from allied sciences. The interconnection of scientific research and technical solutions are thus clearly seen. Despite the obvious topicality and common points of contact, there is no research on the analysis of the CNSS operation and on forecasting incidents [1] in similar systems.

At the same time, there are no models of CNSS functioning and methodological support of the incident identification process in security networks. The objective necessity of methodological generalisation and development of methods and technologies to detect the incidents in the security system operation follows from this unsolved problem.

Thus, modelling of the CNSS operation and process of incident identification in operation of similar complexes is an actual scientific problem.
2. Problem statement

The application of LAN technologies in the CNSS leads to appearance of some essential vulnerability besides obvious advantages in the form of development of the consolidated control tool for all components of security. As the exploitation of this vulnerability can threaten security of people’s lives and health, the task of providing the protection of the CNSS obtains a high priority status.

In most cases, the risks connected to external intrusions are taken into account at the design stage of security networks. At the same time, the probability of internal attacks to accessibility, integrity or confidentiality of CNSS elements is usually assessed as low. The internal attacks include: video camera failure, video recording archive failure, blackout of alarm systems, failure of access card readers, malfunction of communication channels etc.

Susceptibility of information processes of CNSS to security threats defines necessity of constant monitoring and status control of such complexes for the purpose of identification of operation incidents. For the solution of the given problem, it is necessary to introduce a monitoring system of the object status in the CNSS. In such system, data on the equipment status should be collected automatically [2]. The analysis of such information will allow one to provide opportunity of constant development and perfection of a network reliability control system.

As mentioned earlier, the nature of incidents can be various [3]. However, during their occurrence there are always events that are uncharacteristic for the standard operation scenario. This fact allows us to combine various incidents and study them by the nature for consideration in a unified manner. At the same time, regular changes of operating modes can occur in the CNSS. Consideration of all possible scenarios and identification the general laws in practice is not possible not only owing to considerable labour-intensity of the process, but also because of peculiarities of the CNSS functioning.

Nevertheless, recording or identification the moment of uncharacteristic change of the operation scenario during a specific period of time allows one to make an assumption that an incident approaches [4]. The use of mathematical models allowing one to describe the CNSS operation seems logical. Thus, for the solution of the problem of identification of the CNSS operation incidents, it is necessary to obtain the model of the CNSS functioning.

3. Construction of a security network model

Generally, the CNSS structure can be represented in the form of a set of devices and communication channels. Let us represent the CNSS in the form of graph $K$, apexes of which are the devices belonging to a security network, and arches are the communication channels connecting the devices. The present status of the security network can be defined as a set of statuses of all devices composing its structure. Taking into consideration possible scales of the CNSS, modelling a similar complex in the form of a certain set of objects is logical within the limits of a practical task. Such approach allows us to simplify the modelling process and to abstract away from the redundant data that do not influence the result.

Then, the security network can be presented in a form of graph $K'$, apexes of which are the devices chosen to control the network status, and arches are the communication channels connecting chosen devices.

$$K' = (U', M')$$

where $U'$ is a set of the devices chosen to control the network status; $M'$ is a set of the communication channels connecting the controlled devices.

Device $u_i$ possesses a certain set of parameters. Every parameter is characterised by a value that can change in time. Then, the device status in the present moment can be defined as a set of values of all its parameters. Considering the significant number of characteristics of each device, modelling a specific device in the form of a limited set of parameters is logical within the limits of a practical task.

At the stage of the choice of devices and their parameters it is necessary to try to obtain a list of parameters necessary and sufficient for the solution of a certain practical task. If this condition is met, the constructed model and the further decision on classification of the found denial of the system operation are adequate.
Let us define the set of all parameters of device \( u_i \) as set \( P_i \),

\[
P_i = \{ p_{i1}, p_{i2}, \ldots, p_{ik} \}
\]

where \( k \) is the number of parameters of device \( u_i \).

Let us represent device \( u_i \) in the form of the form of set \( P_i' \) – the set of parameters chosen for the control of its status within the limits of the practical task. At that, \( P_i' \subseteq P_i \). Thus, \( |P_i'| \) defines the number of controllable parameters.

At each moment of time \( t_i \), parameter \( p_{ij} \in P_i' \) is characterised by some value \( z \in Z_{ij} \), where \( Z_{ij} \) is a set of all values which can be taken in by the \( j \)-th parameter of an \( i \)-th device.

To define the regular operating mode for each \( p_{ij} \), let us introduce a set of acceptable values \( Z_{ij} \). The problem of formation of set \( Z_{ij} \) will be considered further.

To define the status of device \( u_i \) in present time \( t_i \), it is necessary to check whether all obtained values enter set \( Z_{ij} \).

\[
\text{Criterion} (a,B) = \begin{cases} \text{TRUE, if } a \in B \\ \text{FALSE, if } a \notin B \end{cases}
\]

Let us substitute \( a \) with value \( z \) in function (3). Value \( z \) was obtained when measuring parameter \( p_{ij} \) at time \( t_i \). \( B \) is also substituted with a set of acceptable values \( Z_{ij} \).

Then device status \( s_i \) at time \( t_i \) is defined by logic function (4).

\[
S_i = \text{Criterion} (z_{ij}, Z_{ij}) \land \ldots \land \text{Criterion} (z_{ik}, Z_{ik})
\]

where \( S_i \) is device status \( s_i \); \( z_{ij} \) is the obtained value of parameter \( p_{ij} \).

Let us assume that device \( u_i \) functions normally if \( S_i \) is \( \text{TRUE} \). If \( S_i \) is \( \text{FALSE} \), it means that there is a possible incident in the operation of this device. This moment is marked as \( \text{DENIAL} \) and the process to define whether this \( \text{DENIAL} \) is caused by an incident is started.

In turn, the condition of the normal operation of a security network at time \( t_i \) will be defined by logic function (5).

\[
S = S_1 \land S_2 \land \ldots \land S_i
\]

where \( S \) is the status of the CNSS.

Thus, we believe that at time \( t \) the CNSS works in a regular mode if \( S \) is \( \text{TRUE} \). In cases when \( S \) is \( \text{FALSE} \), there is an assumption of a probable incident in the security network operation.

4. **Application of the model in practice**

For application of the above described model, it is necessary to solve the problem of the set formation of admissible values \( Z_{ij} \) for each device \( u_i \). The authors tried to find an alternative way of criterion formation for the solution of the given tasks, which was considered in detail in [5]. The offered technique of information obtaining allows the operator to choose from the set of devices and parameters that are the most important within the limits of the practical problem being solved to make the choice easier.

Understanding the structure and principles of the CNSS operation allows us to draw the conclusion that the similar complexes represent environment where, during each moment of time, a large quantity of heterogeneous data is generated and processed [6]. Change in time of any of the CNSS parameters forms a time series. Each of such time series represents a certain component of the general status of a network. Denials and failures in the operation directly influence the values of time series [7]. It was defined that at the moment of an incident approach the parameters of observed processes change. In particular, probability of observed events before and after the approach of incident varies [8]. Hence, to reveal an incident, it is necessary to define the moment of uncharacteristic change of the scenario operation with certain probabilistic characteristics.

The offered approach to the solution of the problem of incident identification consists in construction of time series on the basis of data on the values of CNSS parameters and in the
application of the forecasting method to the obtained time series. It is supposed that to reveal an incident it is necessary to form a forecast on the basis of the estimation of the previous values of the investigated parameter and to compare it to the current value.

The developed software “SOWA” [9] was introduced in open joint stock company “Special Technology and Innovation Economic Zone” of Tomsk and was used to control the CNSS consisting of more than 1000 active devices. The video surveillance subsystem is one of the most dynamical components of the investigated CNSS, which is caused by a number of special features of its operation. Besides, the information from the video surveillance cameras is fed to the workstations of the duty staff in a real time mode and is constantly processed by operators. It allows strengthening the control of the investigated object of research and, consequently, increasing the accuracy of the experiment. 3 video surveillance cameras digitalizing the analogue signal from connected video cameras were selected and data were transferred to the server.

The described above features of the system operation connected to the use of various record modes allowed us to make an assumption that the traffic generated by the video surveillance cameras has specific character. There are both constant and variable components of the traffic profile. The constant component is provided by means of data transmission to the server from the video cameras recording constantly. The variable component is specified by data transmission from the video cameras with the “Record on Movement Detection” mode. The intensity increases unevenly due to aperiodicity of the recording.

5. Results of the experiment
The main objective of the experiment is to evaluate the possibility of use of the offered methodological groundwork and of the developed software for identification of the incidents in the CNSS operation on an example of a video surveillance subsystem. The experiment was being carried out during 30 days and consisted in the following. In each watchpost there is a register where operators of video surveillance record all incidents connected to the system operation (irregularities of information display, interference etc.). The register is kept according to strict instructions.

As an alternative to operator’s work, there was an attempt to reveal the incidents on the basis of the forecast of traffic in the network interface of the video surveillance camera to control the system status. As a result of application of the authors’ technique, the traffic generated by the video surveillance camera was controlled. The monitoring system worked irrespective of video surveillance system. To reduce the human factor influence, security guards were not notified about the experiment and continued working according to duty regulations. Inquiries about the amount of traffic in the interface of the video surveillance camera were made every 5 minutes. The data was collected in the storage and was processed by the Holt and Winters method [10].

In case of probable occurrence of an incident the monitoring system sent notifications to the administrator by means of e-mail.

The special feature of the investigated system of video surveillance is the logging subsystem. Besides, the system provides the means to operate the register of events. Within the limits of the experiment, at the end of each day the system administrator possessing the expertise in network equipment and also aware of the features of the investigated object compared the security log entries with the data logging subsystem.

The data received by video surveillance operators was checked by the administrator every day and was verified with the logging system. The obtained result was recorded. To make the analysis complete, the administrator used archive of video surveillance. Similar actions were also carried out for the introduced system of monitoring. The administrator checked the messages of monitoring system about the found incidents every day as well. The incidents confirmed by the administrator were summarised every day and recorded.

The estimation of the received results consisted of two stages:
- the estimation of the work of video surveillance operators as regards the logging subsystem;
- the estimation of monitoring system operation concerning the logging subsystem.
A dispersive analysis was applied to estimate the effect of the means of gathering information on incidents in a CNSS on the result of monitoring with the use of the Fisher criterion. The principal cause of application of the given aspect of the analysis is the possibility to estimate the effect of nonmetering qualitative factor on number indicators.

5.1 Estimation of operators' of activities

Evaluating factor $A$ - a way of data acquisition about incident occurrence in a CNSS was defined. Factor $A$ accepts the following values at an estimation of activity of operators of video surveillance: 1) the work of operators of video surveillance; 2) logging system incidents in the CNSS. Also two statistical hypotheses were generated:

- Zero hypothesis $H_0$: work of operators does not influence the number of the revealed incidents in comparison with logging system (distinctions in the number of the revealed incidents between are not more definite than casual distinctions in each group);

- Alternative hypothesis $H_1$: the effect of work of video surveillance operators has an essential effect on the number of the found incidents in the operation of the CNSS (the number of the incidents revealed by the operator essentially differs from a "reference" indicator - system logging).

Comparison of calculated and tabular values of the criterion showed that in all cases the calculated value of the criterion is more than critical. It means that the difference between dispersions is significant and zero hypothesis about absence of influence of operators work on the number of revealed security incidents should be rejected. In other words, the number of the incidents revealed by the operators essentially differs from data of the logging system processed by the system administrator.

5.2 Estimation of monitoring system functioning

Evaluated factor $A$ - the way of data acquisition on occurrence of incidents in a CNSS was defined. Factor $A$ accepts the following values at the estimation of “SOWA” monitoring system functioning: 1) the application of the monitoring system; 2) the system of logging incidents in the CNSS. Also two statistical hypotheses were produced:

- Zero hypothesis $H_0$: application of the “SOWA” monitoring system does not have an essential effect the number of the revealed incidents in comparison with the logging system;

- Alternative hypothesis $H_1$: the effect of application the “SOWA” monitoring system has an essential effect on the number of the revealed incidents in the CNSS operation in comparison with the logging system.

Comparison of the calculated and tabular values of the criterion showed that in all cases the calculated value is less than critical. It means that the difference between dispersions is insignificant and zero hypothesis about absence of influence of operators work on the number of revealed security incidents cannot be rejected. That is, the difference in the number of the revealed incidents between two specified ways are not more expressed than random difference in each group.

6. Discussion of results

The obtained results show that the number of the incidents revealed by the monitoring system slightly differs from the records in the logging system. At the same time, the number of the incidents recorded by operators considerably differs from a regular logging system.

Considering that the logging system was accepted as a standard and all results of experiment proved to be true by the system administrator of the video surveillance who has an expertise in its operation, it is possible to draw the conclusion about the possibility of use of the developed monitoring system for identification of the incidents.

It is determined that the developed toolkit allows using the offered technique of gathering the information to the full. At the same time tests showed that the monitoring system can be used as an alternative of the detailed studying of the given system logging. In practice, the involvement of the
system administrator to deeply study the logging system data will undoubtedly lead to increase in labour content and consequently to the higher cost of the system operation. The automated system of monitoring that has similar indicators to the ones of an expert should become an alternative. An additional factor characterising the monitoring system positively is the considerable reduction of time needed to detect an incident. In other words, the developed software allows us to improve the status control of the CNSS of an enterprise qualitatively.

7. Conclusion
Construction of complex security system networks has recently become one of the basic directions of people’s life and health protection at enterprises. Despite the topicality of such complexes, the problems of the status control and monitoring remains unstudied. Absence of both models of the CNSS functioning and methodological support of incident identification of operation process is observed.

The purpose of the given research is to fill the gap in the scientific and technical literature lacking the research in the field of modelling of security systems of heterogeneous objects, including the models of functioning and methodological support of the process of incidents identification in operation of such complexes.

The authors defined the features of the CNSS functioning which cause the limited applicability of the status control methods and incident identification methods to them, which are used in a typical LAN. A model of the regular operation of a CNSS is offered and approbation of the approach offered earlier based on detection of uncharacteristic changes in the operating mode of a network was carried out. This approach allows one to generate a logical and time structure of the incident identification process.

The “SOWA” program toolkit is developed. The monitoring system of complex security systems networks allows one to use the offered methodological support of the process of incident identification for strengthening the subsystem status control and to increase the speed of reaction to arising incidents.

8. Acknowledgments
The work was partially supported by the Ministry of Education and Science of the Russian Federation in terms of the basic part of the state order for Tomsk State University of Control Systems and Radiotechnics in 2015–2016 (project № 3657); RFBR (project № 16-47-700350).

References
[1] Lavrova D S and Pechenkin A I 2015 Information Security Problems. Computer Systems 2 80–85
[2] Basov G B, Ostrovskiy E O and Uraskov Y L 2015 Telecommunications 12 16-20
[3] Baranov V A 2011 Information Security Problems. Computer Systems 2 24–31
[4] Fedorchenko A V, Levshun D S, Chechulin A A and Kotenko I V 2016 SPIIRAS Proc. 47 5-27
[5] Iskhakov S Yu, Shelupanov A A and Mescheryakov R V 2014 Proc. Int. Sci. and Tech. Conf. (Omsk) 1–4
[6] Sun S 2015 Int. Conf. Computation on Intelligence and Communication Networks (Jabalpur) pp 1183-87
[7] Kalashnikov A O, Yermilov Y V, Chaporov O N, Razinkin K A, Barannikov N I 2013 World App. Sci. J. 25 (3) 399–403
[8] Homenda W, Jastrzebska A and Pedrycz W 2014 Fuzzy System (FUZZ-IEEE): IEEE Int. Conf. S 1 2055–62
[9] Iskhakov S Yu and Shelupanov A A 2013 Telecommunications 6 16-21
[10] Ekberg J, Ylinen J and Loula P 2011 Int. Conf. for Internet Technology and Secured Transactions (Abu Dhabi) 627-31