Journal of Theoretical and Applied Information Technology
30th June 2020. Vol.98. No 12
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

METHODOLOGY FORMING FOR THE APPROACHES TO THE CYBER SECURITY OF INFORMATION SYSTEMS MANAGEMENT

[1]ADRANOVA A., [2] YONA L., [3]KRYVORUCHKO O., [4]DESIATKO A., [5] PALAHUTA K., [6]BLOZVA A., [7]GUSEV B.

[1] Abai Kazakh National Pedagogical University, Almaty, Kazakhstan,
[2] Distance Learning Institute in O.S. Popov Odessa National Academy of Telecommunications, Department of Cyber Security and Information Security Odessa, Ukraine,
[3,4,5] Kyiv National University of Trade and Economics, Department of Software Engineering and Cybersecurity, Kyiv, Ukraine
[6,7] National University of Life and Environmental Sciences of Ukraine, Kiev, Ukraine

E-mail: [1]assel.adranova@gmail.com, [2]yonalarisa66@gmail.com, [3]kryvoruchko_ev@knute.edu.ua, [4]desyatko@gmail.com, [5]palagutaea@knute.edu.ua, [6]valss725@gmail.com, [7]gusevbs@gmail.com

ABSTRACT

This paper establishes the analogy of displaying an information security management system (ISMS) for information systems (IS) as a queuing system (QS). It became possible through the identification of structural and functional analogies between ISMS and QS. As a result of such analogy, it became possible to model the ISMS as a QS, and subsequently formulate the initial requirements for the ISMS IS. It was defined that the ISMS can be interpreted as a single-phase QS with possible losses. Model for determination of the QS parameters was developed. Due to structural, substantive and functional analogies, newly created models allow one to form range of quantitative ISMS characteristics for IS. This allows one to ensure the effectiveness of the ISMS design process, taking into account the prospects of increasing complexity and the number of destructive effects on IP by attackers. Computational experiments, carried out using a specially designed software application, confirmed the reliability of the main theoretical provisions and practical developments.

Key words: *Information Security Management System, ISMS, Queuing System, QS, Information Protection, Information System, Design Characteristics*

1. INTRODUCTION

Modern information systems (IS) as well as information security management systems (ISMS) for these systems can be characterized by the complex of technical characteristics and architectures as queuing system (QS) [1–3]. Among possible QS schemes in particular with losses, with pending time, with a drive of finite capacity, etc., IS essentially represents systems with mixed priorities and with an unlimited pending time for requests in the queue. In the actual IS operating practice, user requests queue is formed with a transaction mechanism specific for the client-server architectures, see fig. 1.

IS includes following basic elements:
server (s);
Databases (DB);
modules and subsystems:
1) control;
2) information delivery;
3) test tasks generation;
4) administration;
5) information security tools (IST), etc.

Crises in the queue can occur as a result of increase in number of subscribers (IS users) or increase in complexity of requests to the IS (which, in fact, can be result of a usual DoS / DDoS attack). It means that requests will accumulate faster than they can be served. Note that there are dedicated clients in the IS. The latter include, for example, IS administrators or company executives who are served by IS with the highest priority. Necessary to mention that the priority can be artificially modified, for example, as a result of R2L and U2R class attacks. The situations listed above can significantly complicate analyzation and evaluation of the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

necessary mechanisms for IS protection from cyber attacks [4–6].

In practice, various options are used to solve the problems associated with cyber attacks on IS. The most common option is to use a more powerful server, switch to secure OSs, such as Linux, a qualitatively different organization of the company's IS. It is necessary to simulate different situations in order to select the best option for building an IS protection system. Range of following processes: the appearance of new requests from subscribers; duration of transactions in IS; the intensity of IS vulnerabilities exposure; the intensity of IS vulnerabilities detection; the intensity of the identified IS vulnerabilities elimination by the IS staff or by the software developers, can be described by various distribution laws [1,2, 7].

Therefore, it is necessary to keep this fact in mind solving the optimization problem of IST choosing in conditions of the company's or enterprise's limited budget. Additionally, various variants of IS topologies are possible, and, consequently, various statements for the problem of choosing the optimal IST for IS.

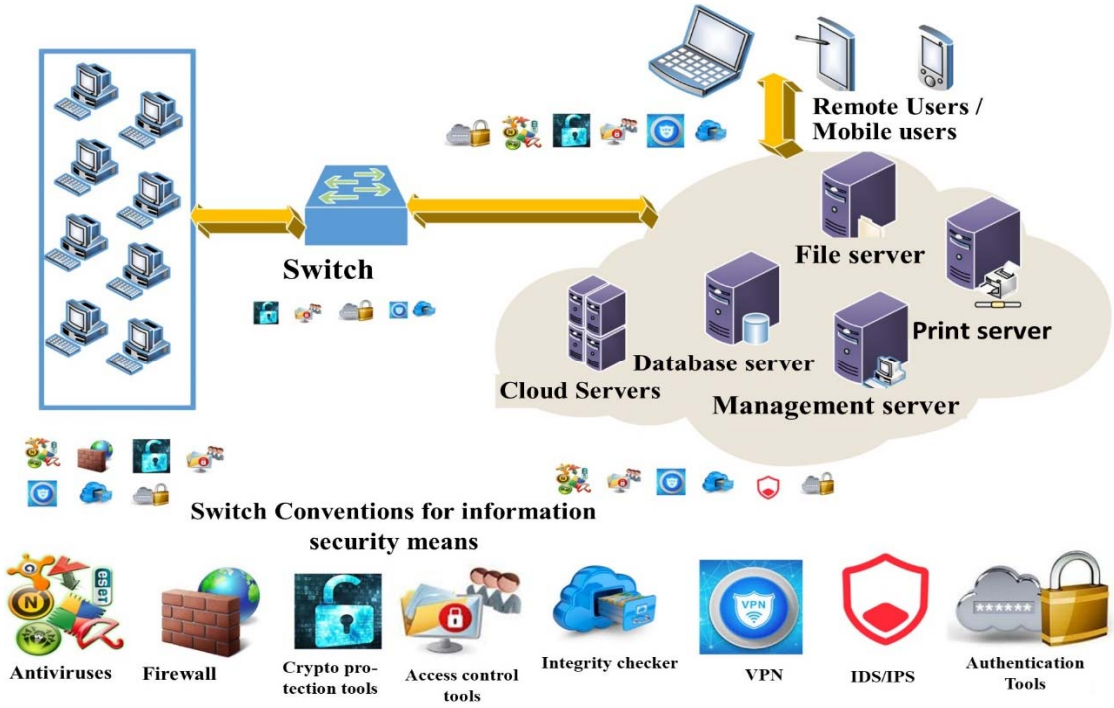

Figure 1 : IS structure with information protection elements

2. THE AIM OF THE ARTICLE

Further development of the model for determination of the information security management system (ISMS) parameters for information systems (IS) as an analogue of the queuing system, which will ensure the effectiveness of the ISMS design process, taking into account the trends of increasing complexity and the number of destructive influences on IS by computer attackers.

3. LITERATURE REVIEW

Analysis and synthesis of organizational and technical information security management systems (ISMS) by the method of functional modeling was considered in [8, 9]. The results obtained in the course of these studies were used as the basis for making decisions on the reconstruction, replacement or development of a new ISMS [8, 9].

In [8, 10], the ISMS is considered in the format of graphical notation IDEF0. The functioning process of such ISMS is being modeled on the example of an institution with the allocation of such functions as entry control, task execution control and monitoring

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11]. Functional modeling of the information technology security assessment process in accordance with the "General Criteria" [12, 13] and the main information security management processes of data flow diagrams (DFD) notation was considered in [11, 15, 14]. Their comparative analysis has been performed and the DFD notation was selected as a higher level technology. Such choice was made due to the study of data flows both in the security of information technology (IT) assessment, and in the context of building an information security management system as a whole [16]. However, authors do not address the issue of functions definition in the ISMS and the sequence of their implementation. In [17, 18], the problem of models, for analyzation of the functional component of an information security object, construction was solved. Moreover, the limits of its functioning were determined and, due to the decomposition of the functional model, its components were analyzed in details. Many of the analyzed works allow one to talk about satisfying the requirements for the process of security of informatization facilities assessment in accordance with the international standard ISO / IEC 15408 provisions.

Functional modeling of the decision support system (DSS) for ensuring the personal data security was performed in [19]. The authors constructed a functional model that allowed one to describe the subject area. As a result, with the help of DSS, an information space for representing knowledge about the protection of personal data was formed. In addition, a functional model of an automated information security management system based on a multi-agent approach has been built [20]. Thanks to this, the data flow in the information system and computer network of the information security object was functionally modeled and investigated.

The study of data flows in IS using functional modeling was also performed in [21]. The model takes into account the functional structure and processes in the IS as well as the interaction between them. In [22], the results of constructing models of an e-commerce system were presented. The model takes into account external threats and allows one to assess risks, as well as obtain an assessment of the e-commerce system security level. The authors do not give practical examples of the implementation of the model.

Studies [1, 2, 5, 8] considered the main qualities of ISMS in order to identify the most common analogies between ISMS and well-known formal systems. The authors conclude that any ISMS can be considered as a class of systems designed for multiple solutions of the same type tasks. This interpretation suggests an analogy between the ISMS and the queuing system (QS), in which the requirements for the performed work are manifested in the form of information security events (ISE). Note that in the general case, the sequence of service requirements, have the form of IS events / risks, is random, both in the time of occurrence of events / risks and in the type of such events / risks. The randomness of the sequence of events / risks served by the ISMS is another aspect of the analogy between the ISMS and the QS.

An increase in the number of IS threats caused a surge in research in the field of effective systems for detecting and preventing cyber attacks development [23, 24], as well as decision support systems (DSS) [14, 18] and expert systems (ES) [15, 19] in this area. The analysis of publications [14, 15, 19, 25] revealed the growing popularity of automated risk assessment tools and information security risk management systems. It was noted in [26, 27] that ISMS, which implements intelligent technologies for identifying cyberattacks and responding to events associated with IS breach, are products of private companies. Therefore, customers in most cases do not possess information regarding methods and models for the formation of control actions in the ISMS.

In addition, according to range of authors [12-14, 17-20], existing standards in the field of management do not form specific approaches to managing cyber security of IS.

Thus, taking into account controversy in the publications [1, 2, 8, 10, 17], the urgent task is the need in development of a new model for information security management system based on the QS model, as well as the development of automation tools for determination of the design characteristics based on computer modeling of various information system states and its ISMS.

4. MODELS AND METHODS

The topology diagram of multichannel QS with mixed priorities and shared buffer memory is shown in Figure 2.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

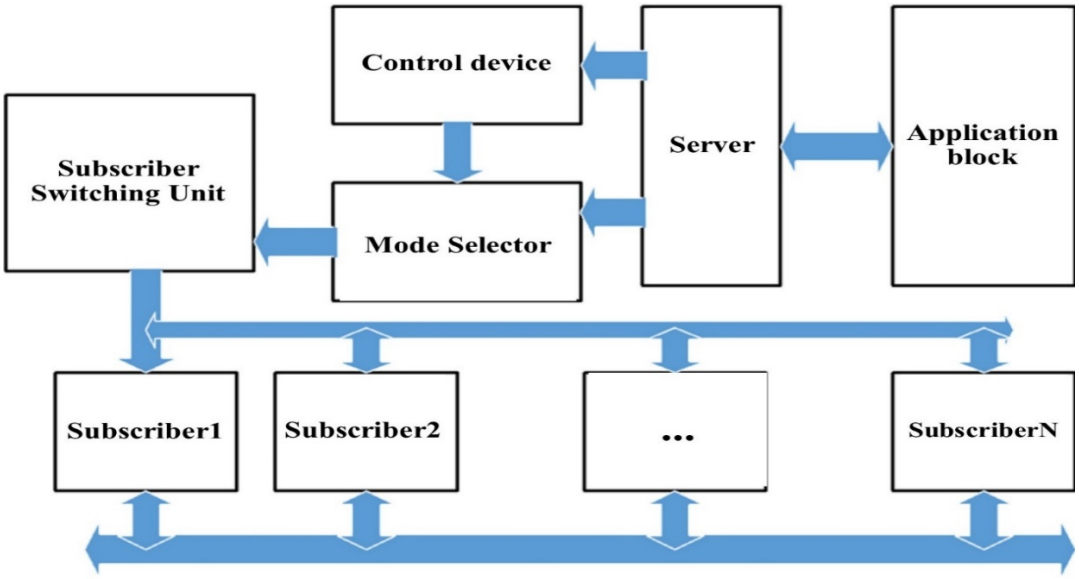

Figure 2 : Functional IS as QS

The scheme shown on Figure 2 functions as following. Requirements (service requests) are sent to the IS server. The server, as the main control device, using the appropriate software and priorities set by the IS administrator, includes a switching unit for subscribers registered in the system or opens guest access. The highest priority can be assigned on the basis of various policies of the information security management system (ISMS) for IS [28]. To ensure information security, leading world companies are implementing information security management systems (hereinafter referred to as ISMS). Such ISMSs are usually built on the basis of the requirements of ISO / IEC 27k. It should be noted that existing standards do not contain specific methodologies that make it possible to uniquely formulate design requirements for the ISMS, as applied to a particular organization. They are rather describing various aspects of information security that should be implemented to protect any business process. In such case, it is desirable to have a formal model describing its functional features in order to select IS security priorities and deploy a functional ISMS.

The study of the parameters for such model will give an understanding of what aspects of information security, in particular, is necessary to pay priority attention. In turn to understand the structure of the formalized ISMS model, one should consider which of the formal methods are more applicable in the course of the ISMS study. If an analogy can be identified, then it can be reasonably assumed that the formal design techniques regulated by the ISO / IEC 27k standards can be adapted to the tasks of creating an ISMS for IS as a whole.

The results of characteristics comparison of the QS processing procedure (PP) and the IS ISMS in order to identify analogies between them are shown in Table 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1 : Comparison of the characteristics of the service mechanism in the QS and ISMS

Description of the mechanism, processing procedures and system structure (Further DM, PP, SS)	**QS**	**Information system ISMS**	**Conclusion**
PP defined by:	PP and SS characteristics	The standard (regulation, instruction) of the organization that describes the sequence of actions for processing information security risks and the structure of the information security unit	Matches (M)
PP	Number of attendants (N)	The number of analysts involved in the processing of information security risks for IS	(M)
	PP duration	The duration of the processing of a single risk of information security	(M)
	Requests are satisfied as a result of each procedure (for group requests)	Requests are received discretely, (Risk information is alternately received)	ISMS has no group requests
	The probability of the serving channel failure	The probability of the serving channel failure	(M)
SS Defined by functioning approach:	Sequential parallel, combined	Sequential, parallel, combined and also, it is possible to attract additional resources	(M)

From the table 1 analysis one can observe the complete coincidence of the service mechanisms of QS and ISMS information system. This, in turn, allows one to find correspondences in the coincident characteristics of the PP of these two types of systems. Structures of processing systems in the ISMS and QS demonstrate full coincidence, although they use slightly different working methods. In addition, we note that the time for processing requests (processing cybernetic risks associated with overcoming IS protection loops) depends on the nature of the requests themselves or on customer requirements. Such requirements, for example, include the maximum value of cybernetic risk (CR); the time required to carry out activities for its analysis and processing of CR; from the state and capabilities of the organization's processing systems (information security division or individual information security specialist). In some cases, it may also be necessary to take into account the parameters of the probability of failure of the serving channels, for example, after a certain limited time interval. This characteristic of the QS can be modeled as a failure flow, which takes precedence over all other requests. Similar reasoning is quite acceptable for ISMS [1].

Based on a detailed analysis of the QS structure and its functional model details, a structural-functional analogy between the QS and ISMS IS was established during the study. In particular, the basic elements of these systems can be compared and similar problems solved using the provisions of queuing theory (QT). In a first approximation, the ISMS IS can be considered as a single-phase QS with possible failures.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Consideration of the interpreting possibility for the main characteristics of the QS (the service mechanism, the structure of the service system, the characteristics of the PP) in the context of the ISMS revealed their complete coincidence. The analogy of systems makes it possible to use the mathematical apparatus and well-known calculation methods inherent in QS while designing ISMS [29, 30].

As an example, for further studies in order to determine the design characteristics of the ISMS IS, the differential equations of the QS were used. Let us consider a simple case when there should not be more than one risk in the ISMS queue, for example, the risk of a DoS / DDoS attack

Let us denote S_i - the state of the ISMS IS in which there is a queue of i $(i = 0,1,2, ...)$ risks at the input of the ISMS that must be processed. The probability that at the time t at the entry to the ISMS there is a queue of i risks, one denote by $p_i(t)$. In other words, $p_i(t)$ is the probability that the ISMS is in a state S_i. Let us assume that for an ISMS, at the entry of which we have a queue of i risks, the intensity of the risk flow and the intensity of risk processing depend on the length of the queue, that means $\lambda = \lambda_i$ and $\mu = \mu_i$, accordingly.

It is necessary to build a model of probability change $\Delta p_i(t)$ over a period of time Δt, immediately after the moment t.

Then the corresponding pair of differential equations will look like following [1, 30, 31–33]:

$$\frac{dp_0(t)}{dt} = -\lambda_0 * p_0(t) + \mu_1 * p_1(t), \quad (1)$$

$$\frac{dp_1(t)}{dt} = \lambda_0 * p_0(t) - \mu_1 * p_1(t). \quad (2)$$

If one supply this pair of equations with the total probability relation:

$$p_0(t) + p_1(t) = 1, \quad (3)$$

then the three above written relations represents the Kolmogorov system of equations for the probabilities of the state of a single-channel QS with service failures.

In the Poisson flow of risks for IS, the initial conditions for this system of equations will be following values $p_0(0) = 1$, and $p_1(0) = 0$

And its solution will be the following relationships:

$$p_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}; \quad (4)$$

$$p_1(t) = \frac{\mu}{\lambda+\mu} - \frac{\lambda}{\lambda+\mu} e^{-(\lambda+\mu)t}. \quad (5)$$

From these relations it follows that at the $t \to \infty$ limiting stationary mode of the ISMS IS will be characterized by the following probability values:

$$p_0(t) = \frac{\mu_1}{\lambda_0+\mu_1}; \quad (6)$$

$$p_1(t) = \frac{\lambda_0}{\lambda_0+\mu_1}. \quad (7)$$

Thus, the above substantiates the analogy of displaying the ISMS as a queuing system. This became possible due to identification of structural and functional analogies between them. Among them, the input flow of requests (risk processing) for processing, the discipline of the queue and the service mechanism were highlighted. According above written, the ISMS IS can be interpreted as a single-phase QS with failures.

To implement the models described above, a software product was developed for modeling the ISMS parameters as a QS. This software product allow one to visualize requests to IS servers during computational experiments, as well as simulate the dynamics of request intensities, for example, during external and internal DoS / DDoS attacks. DoS / DDoS attacks as a modeling object of impact on IS were selected based on the statistics of their use against IS, and also on the basis that the implementation of such attack does not require highly skilled attackers [3, 4]. Although the economic damage from such attacks is quite noticeable for any organization.

Figures 3-5 represents the main interfaces of the "ModelSMO2020" software product (SP) for modeling various operating modes of an IS and its ISMS as a QS.

One of the functions fragment for ISMS states modelling is presented in Annex 1. The program was implemented using the algorithmic language Delphi.

Journal of Theoretical and Applied Information Technology
30th June 2020. Vol.98. No 12
© 2005 – ongoing JATIT & LLS
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

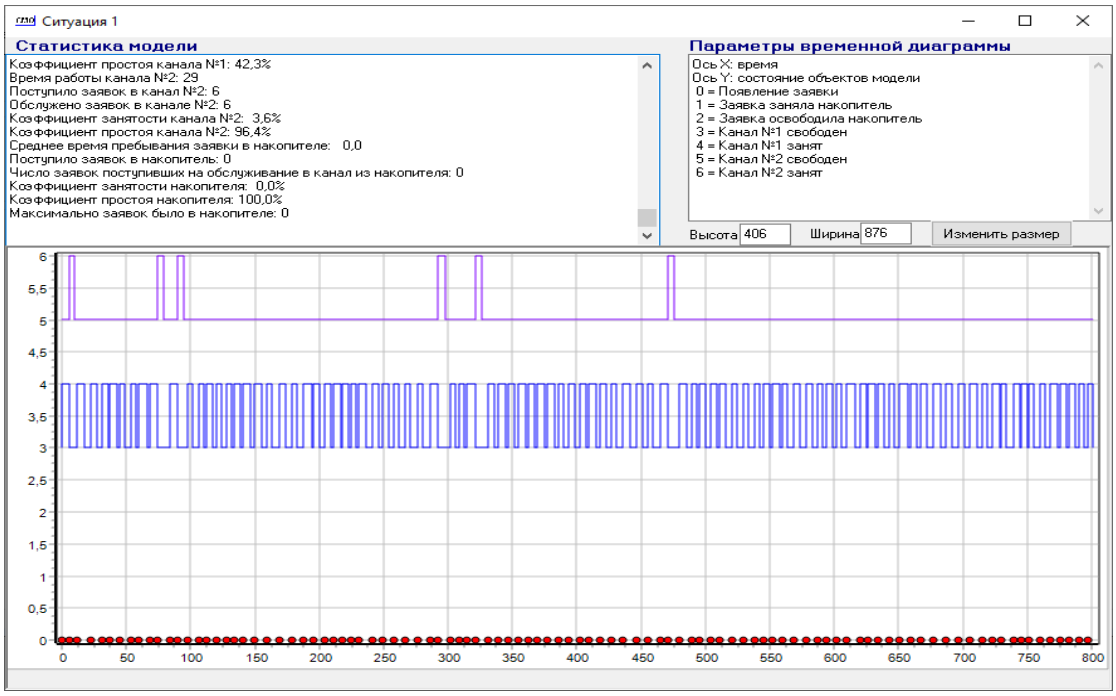

Figure 3 : Modeling of the requests receipt in IS and its ISMS, distributed according to a uniform law

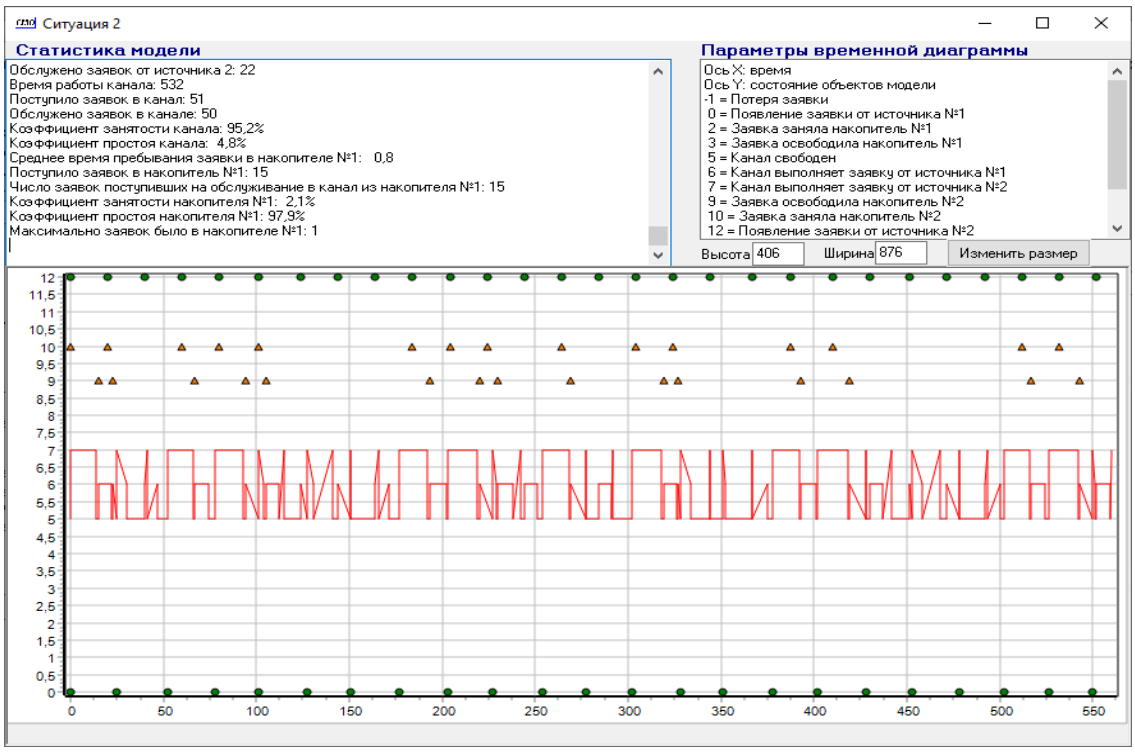

Figure 4 : The results of situation modeling with the requests to IS and its ISMS according to the exponential distribution law and requests in which one of the flows have a higher priority

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

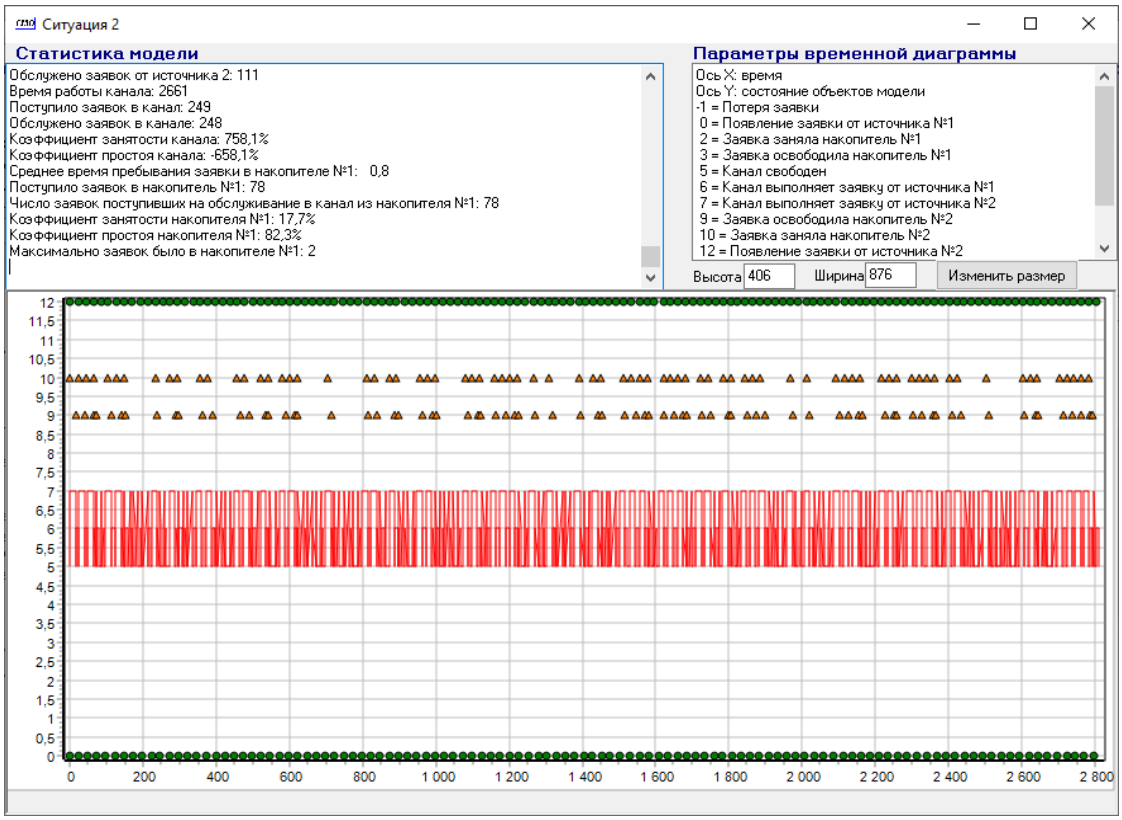

Figure 5 : The results the situation modeling with requests to IS and its ISMS according to the exponential distribution law and requests in which one of the flows have a higher priority (The channel is busy with a busy factor of 758% as a result of an attack on the IS server)

On figures 3–5, broken lines represents distribution density function graphs of received requests. Colored markers (triangles and points) represents, respectively, the variance and order values located in the serving channels.

As it can be seen from the results of modeling the operating modes of the IS and its ISMS as a QS, if the distribution law of the input stream of requests is uniform or normal, then deviations from the standard modes of the system cannot be observed. However, if one assigns a higher priority to one of the flows (Fig. 3), then the situation will radically change. That means that the usual configuration of the IS server, designed, for example, for the intensity of requests not more than 20–70 requests per second, will not be able to provide normal request processing service. And already at 100–120 requests per second with a single server, the load factor will reach 700–800%.

It is also shown that the exponential law leads to the greatest dispersion of the output. Moreover, this dispersion does not depend on the intensity values of the incoming requests flow.

Similar calculations were performed for the ISMS simulation situation based on the dependencies shown in Table 2. That means that the proposed software for modeling the ISMS design characteristics has advanced functionality. In particular, software can provide automation of the ISMS characteristics values of calculation and can be used to make decisions on risk management in the design of ISMS with a complex architecture of a distributed computing network.

An experimental study was carried out for the risk level values of overcoming IS information protection loops in the range $0{,}0001 < r_0 < 1$ for a given intensity of the service flow and the expected risk processing time expressed in one conventional unit of time. The results were formed in the form of a database of design characteristics indicators, which allows one to ensure the effectiveness of the ISMS design process.

An example of calculating the ISMS parameters for $r_0 = 0{,}9;\ \mu = 1$ is given in Table 3. The correctness of the ISMS display as a QS is shown. For this, the input risk flow is considered as Poisson with the intensity λ. This means that risks arise at random times, and the probability of one risk in the time interval $(t, t + \Delta t)$ does not depend on time t and is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

equal to $\lambda\Delta t$. While the probability of occurrence in this time interval of two or more risks associated with an attack on the IS is very small. The processing time of individual CRs is assumed to be random with an exponential distribution law and average processing time $1/\mu$.. This means that the probability of completing the processing of the next CR in the time interval $(t, t+\Delta t)$ does not depend on the time instant and is equal to $(\mu \cdot \Delta t)$.

Table 2 : Formation of design requirements for ISMS IS Based on materials [1, 2, 6, 30, 31, 36–41]

Design characteristic of ISMS IS	Analytical presentation of the IS ISMS characteristics
Intensity of the service flow μ, processing time $t_{processing}$, nominal performance of the ISMS IS.	$t_{processing} = \frac{1}{\mu}$
IS ISMS load intensity ρ.	$p = \frac{\lambda}{\mu}$
The probability that the ISMS IS does not handle the risk p_0, (the proportion of the ISMS IS idle time), the relative throughput Q.	$p_0 = \frac{\mu}{\lambda+\mu}Q$
The probability of failure $p_{failure}$ in the processing of risk for IS, the average number of risks that can be processed per unit time L_{proc}.	$p_{failure} = \frac{\lambda}{\lambda+\mu} = L_{proc}$
Absolute throughput A (intensity of the flow of served requests in the ISMS).	$A = \frac{\lambda\mu}{\lambda+\mu}$
The average idle time of the ISMS t_{idle}.	$t_{idle} = \frac{\lambda}{\mu(\lambda+\mu)}$
The number of information security risks for IS that are denied for future processing per unit of time.	$\frac{\lambda * \lambda}{\lambda+\mu}$

Table 3 : Design of ISMS information system characteristics with a certain acceptable level of risk of overcoming information security loops

Parameter	Conditional designation	Value
Time of processing	t	1
The intensity of the flow of cybernetic risks (hereinafter CR) for IS	λ	0,0052
CR processing flow rate in ISMS	μ	1
ISMS load rate	p	0,005
ISMS idle state probability	p_0	0,995
ISMS average idle state duration	$t_{downtime}$	0,0052
The share of untreated CR	P_{unproc}	0,0052
ISMS Absolute Bandwidth	A	0,006
ISMS Relative Bandwidth	Q	0,995
Average number of CRs processed by the ISMS	L_{proc}	0,0052

Thus, comparison of the possibilities for interpreting the characteristics of the proposed ISMS model for IS as QS with previously known models proves that such realisation of the ISMS provides greater efficiency of the design process by increasing the reliability of the interpretation of the level of acceptable cybernetic risk in the design characteristics of the ISMS due to other formal requirements (quantitative design characteristics) [34–39].

Thus, in contrast to similar scientific works in the same field [16, 18, 22, 26, 30, 42–45], this research identifies a set of queuing systems (QMS) models, for the first time. Moreover, due to analogies of structural, meaningful and functional characteristics of defined models set made it possible to form a set of quantitative characteristics for the information security management system (ISMS), that in turn allows one to ensure the efficiency of the ISMS design process. For the first time, software products that use the ISMS model as a QMS model were proposed. These products allow one to determine the level of risks acceptability for further decision-making on their management in course of ISMS designing.

Conducted computational experiments have confirmed the reliability of the main theoretical principles, practical developments and conclusions made in the study.

5. CONCLUSIONS

The following results were obtained in the work:

• an analogy was established for displaying an information security management system for information systems (IS) as a queuing system (QS). It became possible due to the identification of structural and functional analogies between IS and QS. It was shown that a consequence of such an interpretation may be the possibility of modeling and forming the initial requirements for ISMS IS as a QS. It was shown that the ISMS can be interpreted as a single-phase QS with failures;

• further model for the QS parameters determination was developed, which, due to structural, substantive, functional analogies, allow one to generate a lot of quantitative characteristics of the ISMS for IS, moreover it allows one to ensure the effectiveness of the ISMS design process taking into account the prospects of increasing complexity and the number of destructive effects on IS from computer intruders;

• an interpretation of the ISMS characteristics for IS as an QS was given. It was shown that such a formalized ISMS model provides greater efficiency for the design process by increasing the reliability of the results of interpreting the level of acceptable cyber risk into the ISMS design characteristics by obtaining other formal requirements (quantitative design characteristics);

• computational experiments were carried out, and they confirmed the reliability of the main theoretical provisions and practical developments.

REFERENCES:

[1] Mokhor, V.V., Bakalinskij, O.O., Czurkan, V.V. (2017). “Deskriptivny`j analiz analogij mezhdu sistemami upravleniya informaczionnoj bezopasnosti i sistemami massovogo obsluzhivaniya”, *Zakhist Informaczii*, 19(2), pp.119–126.

[2] Mokhor, V.V., Bakalinskij, O.O., Czurkan, V.V. (2018). “Analiz sposobov predstavleniya oczenok riskov informaczionnoj bezopasnosti”, *Information technology and security*, vol. 6, pp. 75-84.

[3] Mokhor, V.V., Bakalinskij, O.O., Czurkan, V.V. (2018). “Predstavlenie oczenok riskov informaczionnoj bezopasnosti kartoj riskov”, *Information technology and security*, vol. 6, pp. 94-104.

[4] Lakhno, V.A. (2020). Algorithms for Forming a Knowledge Base for Decision Support Systems in Cybersecurity Tasks, *Advances in Intelligent Systems and Computing*, 938, pp. 268–278.

[5] Adranova, A. et al. (2019). Modeling of cyber threats in information networks of distance education systems, *Journal of Theoretical and Applied Information Technology*, 97 (18), pp. 4921–4933.

[6] Akhmetov, B.S., Akhmetov, B.B. et. al. (2019). Adaptive model of mutual financial investment procedure control in cybersecurity systems of situational transport centers, (2019) *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*, 3 (435), pp. 159–172.

[7] Lakhno, V., Boiko, Y., Mishchenko, A. et Al. (2017). Development of the intelligent decisionmaking support system to manage cyber protection at the object of informatization, *Eastern-European Journal of Enterprise Technologies*, 2 (9-86), pp. 53–61.

[8] Akhmetov, B., Korchenko, A., Arkhipov, A., Kazmirchuk, S. (2018). Postroyeniye sistem analiza i otsenivaniya riskov informatsionnoy bezopasnosti. Teoriya i prakticheskiye resheniya. Monografiya. V 2-kn. Kn.1. Aktau: redaktsionno-izdatelskiy otdel KGUTI im. Sh. Esenova, 387 p.

[9] Lakhno, V., Kozlovskyi, V., Boiko, Y., Mishchenko, A., Opirskyy, I. (2017). Management of information protection based on the integrated implementation of decision support

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

systems, *Eastern-European Journal of Enterprise Technologies*, 5 (9-89), pp. 36–42.

[10] Atymtayeva, L., Kozhakhmet, K., Bortsova, G. (2014). Building a Knowledge Base for Expert System in Information Security, Chapter Soft Computing in Artificial Intelligence Vol. 270 of the series Advances in Intelligent Systems and Computing, pp. 57–76.

[11] Kanatov, M., Atymtayeva, L., Yagaliyeva, B. (2014). Expert systems for information security management and audit. Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 15th International Symposium on 3–6 Dec. 2014, pp. 896 – 900.

[12] ISO 31000:2018. Risk management. Guidelines. [Effective from 2018-02-15]. Geneva, 2018, 16 p.

[13] BSI-Standard 200-1:2017. Managementsysteme für Informationssicherheit [Online]. Verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_1.html Zugriff am: Juni 15, 2019.

[14] Akhmetov, B. et al. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity, *Eastern-European Journal of Enterprise Technologies*, 1 (2–85), pp. 4–15.

[15] Lakhno, V.A., Kravchuk, P.U., Pleskach, V.L. et al. (2017). Applying the functional effectiveness information index in cybersecurity adaptive expert system of information and communication transport systems, *Journal of Theoretical and Applied Information Technology*, 95 (8), pp. 1705–1714.

[16] Lakhno, V., Akhmetov, B., Malyukov, V., Kartbaev, T. (2018). Modeling of the decision-making procedure for financing of cyber security means of cloud services by the medium of a bilinear multistep quality game with several terminal surfaces, *International Journal of Electronics and Telecommunications*, 64 (4), pp. 467-472.

[17] Kearney, W., Kruger, H. (2015). Theorising on risk homeostasis in the context of information security behaviour, *Information and Computer Security*, Vol. 24 Iss: 5.

[18] Akhmetov, B., Lakhno, V. (2018). System of decision support in weaklyformalized problems of transport cybersecurity ensuring, Journal of Theoretical and *Applied Information Technology*, 96 (8), pp. 2184–2196.

[19] Li-Yun, Chang, Zne–Jung, Lee (2013). Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, 2013 International Conference on Fuzzy Theory and Its Applications (iFUZZY), pp. 346 – 351.

[20] Lakhno, V., Buriachok, V., Parkhuts, L., et al. (2018). Development of a conceptual model of adaptive access rights management with using the apparatus of petri nets, International Journal of Civil Engineering and Technology, 9 (11), pp. 95–104.

[21] Lakhno, V.A., Kasatkin, D.Y., Blozva, A.I., Gusev, B.S. (2020). Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University, *Advances in Intelligent Systems and Computing*, 938, pp. 600–609.

[22] Niranjanamurthy, M., Kavyashree, N., Jagannath, S., & Chahar, D. (2013). Analysis of e-commerce and m-commerce: advantages, limitations and security issues. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(6), 2360–2370.

[23] Akhmetov, B. et al. (2019). Development of sectoral intellectualized expert systems and decision making support systems in cybersecurity, *Advances in Intelligent Systems and Computing*, 860, pp. 162–171.

[24] Lakhno, V., Kartbaev, T., Doszhanova, A., Malikova, F., Alimseitova, Z., Tolybayev, S., Sydybaeva, M. (2019). Algorithm and Improved Methodology for Clustering Data with Self-learning Elements for Intrusion Detection Systems, *Advances in Intelligent Systems and Computin*g, 1046, pp. 165–173.

[25] Lakhno, V., Petrov, A., Petrov, A. (2018). Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport, *Advances in Intelligent Systems and Computing*, 656, pp. 113–127.

[26] Lakhno, V. (2016). Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering, *Eastern–European Journal of Enterprise Technologies*, Vol. 2, No 9(80): Information and controlling system, pp. 18–25.

[27] Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security, *International Journal of Information Security Science*, Vol. 1, No 1, pp.13–19.

[28] Lakhno, V., Akhmetov, B., Korchenko, A., Alimseitova, Z., Grebenuk, V. (2018). Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity, *Journal of Theoretical and Applied Information Technology*, 96 (14), pp. 4530–4540.

[29] Chen, P. Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS quarterly*, 397-422.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[30] Durowoju, O. A., Chan, H. K., & Wang, X. (2011). The impact of security and scalability of cloud service on supply chain performance. *Journal of Electronic Commerce Research*, *12*(4), pp. 243–256.

[31] Lakhno, V.A., Tretynyk, V.V. (2019). Information technologies for maintaining of management activity of universities, Advances in Intelligent Systems and Computing, 754, pp. 663–672.

[32] Lakhno, V., Kryvoruchko, O., Mohylnyi, H., Semenov, M., Kiryeyev, I., Matiievskyi, V., Donchenko, V. (2019). Model of indicator of current risk of threats realization on the information communication system of transport, *International Journal of Civil Engineering and Technology*, 10 (2), pp. 1–9.

[33] Abuova, A., et al. (2019). Conceptual Model of the Automated Decision-Making Process in Analysis of Emergency Situations on Railway Transport, Lecture Notes in Business Information Processing, 375 LNBIP, pp. 153–162.

[34] Kartbayev, T., et al. (2019). Development of decision support system based on feature matrix for cyber threat assessment, 2019) *International Journal of Electronics and Telecommunications*, 65 (4), pp. 545–550.

[35] Akhmetov, B., et al. (2019). Models and algorithms of vector optimization in selecting security measures for higher education institution's information learning environment, *Advances in Intelligent Systems and Computing*, 860, pp. 135–142.

[36] Lakhno, V., Tsiutsiura, S., Ryndych, Y., Blozva, A., Desiatko, A., Usov, Y., & Kaznadiy, S. (2019). Optimization of information and communication transport systems protection tasks. *International Journal of Civil Engineering and Technology*, *10*(1), 1–9.

[37] Borowik, B., Karpinskyy, M., et al. (2013). Digital and Analog Quantities (Book Chapter), *Intelligent Systems, Control and Automation: Science and Engineering*, Volume 63, pp. 1–7.

[38] Borowik, B., Karpinskyy, M., et al. (2013). Number Systems, Operations, and Codes (Book Chapter), *Intelligent Systems, Control and Automation: Science and Engineering*, Volume 63, pp. 9–18.

[39] Borowik, B., Karpinskyy, M., et al. (2013). Error Correction in Digital Systems (Book Chapter), *Intelligent Systems, Control and Automation: Science and Engineering*, Volume 63, pp. 37–43.

[40] Lakhno, V., Malyukov, V., et al. (2020). Model of cybersecurity means financing with the procedure of additional data obtaining by the protection side, *Journal of Theoretical and Applied Information Technology*, Vol. 98, Iss. 1, pp. 1–14.

[41] Akhmetov, B. et al. (2019). Developing a mathematical model and intellectual decision support system for the distribution of financial resources allocated for the elimination of emergency situations and technogenic accidents on railway transport, *Journal of Theoretical and Applied Information Technology*, Vol. 97, Iss. 16, pp. 4401–4411.

[42] Lakhno, V., Matus, Y., Malyukov, V., Desyatko, A., Hnatchenko, T. (2019). Smart City Cybersecurity Projects Financing Model in Case of Description of Investors' Resources with Fuzzy Sets, *2019 IEEE International Conference on Advanced Trends in Information Theory*, ATIT 2019. pp. 249–252.

[43] Lakhno, V., Kasatkin, D., Blozva, A. (2019). Modeling cyber security of information systems smart city based on the theory of games and Markov processes, 2019 IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology, PIC S and T 2019, pp. 497–501.

[44] Valeriy, L., Volodymyr, M., Olena, K., Mykola, T., Alyona, D., Tetyana, M. (2020). Model of Evaluating Smart City Projects by Groups of Investors Using a Multifactorial Approach, Communications in Computer and Information Science Vol. 1193 CCIS, 1st International Conference on Applied Technologies, ICAT 2019, pp. 13–26.

[45] Borowik, B., Karpinskyy, M., Lahno, V., Petrov, O. (2013). Minimizing Boolean Functions, (Book Chapter), *Intelligent Systems, Control and Automation: Science and Engineering*, Volume 63, pp. 75–100.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
procedure TFrZad1.Button1Click(Sender: TObject);
var i:byte; p:real;
begin
FrZad1Statistica.Init;
FrZad1Statistica.Show;
FrZad1Statistica.Memo1.Clear;
GlobalTime:=0;
G:=TGenerate.Create;
G.Init('Источник_1',0,strtoint(Edit2.Text)-1,strtoint(Edit3.Text));
K:=TKanal.Create;
if CheckBox1.Checked then
 begin
  K.Init('Channel_1',strtoint(Edit4.Text),true,0,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));
  K.N.Init('Drive_1',strtoint(Edit7.Text));
 end else K.Init('Channel_1',strtoint(Edit4.Text),false,0,strtoint(Edit5.Text)-1,strtoint(Edit6.Text));
FrZad1Statistica.Memo1.Lines.Add('MODELLING_PARAMETERS');
if RadioButton1.Checked then FrZad1Statistica.Memo1.Lines.Add('Condition for model termination: Time='+Edit1.Text)
 else FrZad1Statistica.Memo1.Lines.Add('Condition for model termination:  Served requests quantity='+Edit1.Text);
FrZad1Statistica.Memo1.Lines.Add('Requests Source: Time='+Edit2.Text+' Accuracy='+Edit3.Text);
if CheckBox1.Checked then FrZad1Statistica.Memo1.Lines.Add('Channel: Quantity='+Edit4.Text+
                                ' Time='+Edit5.Text+' Accuracy='+
                                Edit6.Text+' Has Drive=yes '+
                                Capacity='+Edit7.Text) else
  FrZad1Statistica.Memo1.Lines.Add(Channel: Quantity='+Edit4.Text+' Time='+Edit5.Text+' Accuracy='+
            Edit6.Text+' Has Drive=no);
FrZad1Statistica.Memo1.Lines.Add('MODELING STARTED!');

//---------------------------------------------------------------------------
repeat
if CheckBox2.Checked then FrZad1Statistica.Memo1.Lines.Add('Текущее время = '+inttostr(GlobalTime));
if G.Run then                    {=new request appearance=}
 begin
  if CheckBox3.Checked then
   begin
    FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Request Appearance.'+
    ' Total requests='+inttostr(G.AllCount)+
    ' Next request time='+inttostr(G.NextTimeRun));
   end;
  FrZad1Statistica.Series1.AddXY(GlobalTime,0);
 end;

if G.Zayavka>0 then                {=Budy channels=}
 begin
  K.ZayavkaIn(false);
  if (K.InKanal=false)and(K.InNakopitel=false) then
   begin
    G.ZayavkaOut(true);
    FrZad1Statistica.Series4.AddXY(GlobalTime,-1);
   end else G.ZayavkaOut(false);
 end else K.ZayavkaIn(true);

if CheckBox7.Checked and K.KanalFromNakopitel then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+
  '= Request released the drive. Requests in the drive='+
  inttostr(K.N.Emkost)+' Total request releases='+inttostr(K.N.ZayavkaRun));
 end;
if K.KanalFromNakopitel then
 begin
  FrZad1Statistica.Series3.AddXY(GlobalTime,2);
 end;
if CheckBox6.Checked and K.InNakopitel then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+
  '= Request assigned to the drive. Requests in the drive='+
  inttostr(K.N.Emkost)+' Total requests received='+inttostr(K.N.AllCount));
 end;
if K.InNakopitel then
 begin
  FrZad1Statistica.Series2.AddXY(GlobalTime,1);
 end;
if CheckBox4.Checked and (K.InKanal or K.KanalFromNakopitel) then
 begin
  FrZad1Statistica.Memo1.Lines.Add('='+inttostr(GlobalTime)+'= Channel № is busy'+
  inttostr(K.KanalNFree)+'. Total requests received='+inttostr(K.AllCount)+
  '. Processing time for current request='+inttostr(K.NextTimeRun[K.KanalNFree]));
 end;
if K.InKanal or K.KanalFromNakopitel then FrZad1Statistica.DownUpDown;
```

Annex 1- One of the functions fragment for ISMS states modelling