Int. J. Communications, Network and System Sciences, 2020, 13, 161-169
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Development of an Analytical Model of the Process of Cybersecurity Protection of Distributed Information Systems of Critical Infrastructure

Ramaz R. Shamugia[1,2]

[1]Ilia Vekua Sokhumi Institute of Physics and Technology, Tbilisi, Georgia
[2]Sokhumi State University, Tbilisi, Georgia
Email: rmz.shamugia@gmail.com

How to cite this paper: Shamugia, R.R. (2020) Development of an Analytical Model of the Process of Cybersecurity Protection of Distributed Information Systems of Critical Infrastructure. *Int. J. Communications, Network and System Sciences*, **13**, 161-169.
https://doi.org/10.4236/ijcns.2020.1310010

Received: September 12, 2020
Accepted: October 28, 2020
Published: October 31, 2020

Abstract

This article is dedicated to the creation of the analytical model of quantitative estimation of cybersecurity of Information Systems of Critical Infrastructure (ISCI). The model takes into consideration the existence, in the discussed ISCI, of both the intelligent tools of detection, analysis and identification of threats and vulnerabilities and means for restauration and elimination of their consequences. The development of the model also takes into consideration probabilistic nature of flow of events happening in ISCI and transferring the system between different states of cybersecurity. Among such probabilistic events we mean any operational perturbations (that can cause extreme situations) happening in ISCI under the influence of cyber-threats, as well as events concerning restoration and elimination of consequences of such cyber-threats. In this work, as methods of modelling, there have been used methods of system-oriented analysis based on theory of probability, theory of reliability and theory of queues. These methods enabled to describe analytically dependence of effectiveness indices of ISCI operation on abovementioned probabilistic processes.

Keywords

Cyberspace, Critical Infrastructure, Multichannel Queuing System, Cybersecurity, Cybersecurity Protection System

1. Introduction

It is known that the fast development of information technologies and their pe-

netration into all fields of human activities as well as globalization processes happening everywhere in the world, and where as information systems of the whole world are merged into one entity that is called the global information space cyberspace, all these necessitate to provide them with guaranteed protection from negative external impacts.

In the abovementioned cyberspace, due to complex structures and the nature of interaction between elements of complex information systems, analysis of their effective operation by means of traditional methods is not always effective.

As examples of such complex systems can be named information systems of management console in different fields like energy industry, telecommunication and transport nets, credit and financial systems, different information systems designed for state or military use, and they are spatially-allocated in multicomponent structures called critical infrastructure—CI.

The necessity to settle practical calculations concerning different kinds of possible consequences, undesired cyber impacts on the critical infrastructure—CI, these all demand development of the whole hierarchy of complex mathematical models that are able to describe accurately enough and take into consideration complex impact on the system, both destabilizing factors (like refusals, vulnerability, threats, attacks etc.) and stabilizing ones (like discovery, restauration, elimination, prevention of consequences of cyber-incidents, their blocking out, interruption, localization etc.)

Modelling of processes of critical infrastructure operation exposed to different outer impacts and at the same time having within itself means of detection and prevention their consequences, are widely used while providing information security and cybersecurity [1]-[8].

Generally, on the basis of these models, the level of protection of an object is analyzed and criteria of effectiveness for means of protection are chosen, methodology and regulations for cyber-incident responses are developed.

2. The Object, Aim and Methods of Investigation

Keeping in mind the urgency of the problem mentioned above, in this article, there has been defined the object, aim and methods of investigation:

The object of investigation: multichannel queueing system whose every channel is multichannel QS with limited queues that contains in its body tools of command, control and restoration of subchannels.

The Purpose of the Research: the development of operation models of information systems of critical infrastructure takes into consideration the presence of intelligent tools of detection, analysis and identification of threats and vulnerabilities with the ability to restore their consequences. The development of the models in question takes into consideration probabilistic nature of events flow happening in ISCI and transferring them between different states of cybersecurity.

Methods of research: there have been used systems analysis methods based

on using Theory of Probability, Theory of Reliability and Theory of Queues that enable to describe analytically probabilistic processes of cybersecurity violations in IS of critical infrastructures caused by realization of cyber-threats that can cause extreme situations in them and processes of restoration or elimination of their consequences.

The idea of research conducted in this work is to create an analytical model for evaluating of cybersecurity level of complex information systems that enables to estimate the quality of their work by defining values of main characteristics of effective operation in case of different values of input parameters and by means of their comparative analysis to provide choices of the best variants of such systems as in the process of project development as well as for the organization of the processes of their rational exploitation.

Precondition to this particular work have been researches conducted in the works [9]-[14] where special role of modelling in security provision of ISCI is justified, there are also discussed possible types of vulnerabilities taking place in them, there is given classification of threats, methodological concepts for neutralizing those threats on the basis of complex of measures for security and stable functioning of objects and subjects of ISCI from extreme situations caused by these impacts.

This research was also preceded by the author's articles concerning the developments of analytical and simulation models of complex technical systems regarded as multichannel queueing systems, published in the works [15]-[20].

3. Statement of the Problem

The pictures given below show schematic diagrams of the following objects substituting investigated ISCI:

- Multichannel queuing system with limited queue taken as the basis of every channel considered as unified complicated QS with the illustration of its corresponding state transition graph (**Figure 1**).
- Investigated multichannel QS, whose every channel is presented as QS given on **Figure 1**, with the tools of immediate queue discipline, enhanced with the tools of command and control of channels, as well as tools of restoration and elimination of consequences of cyber-impacts (**Figure 2**).

The aim of this investigation is creation of mathematical model connecting input parameters and output characteristics of the investigated system and providing with ability to oversee their interdependence in the modelling process.

4. The Parameters of the Investigated System

In reference to the parameters of the structure of the information system in question, the following assumptions are made:

- Cyber threats are being divided in the system according to the status: detected and sent for restoration; detected but waiting for restoration (in the virtual queue).

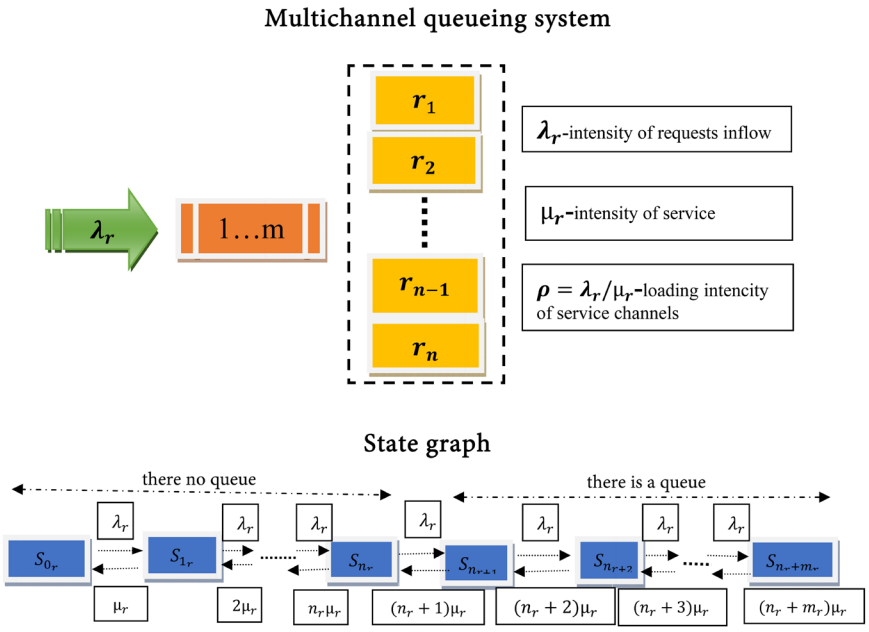

Figure 1. Block diagram of a multi-channel Queuing system with a limited queue.

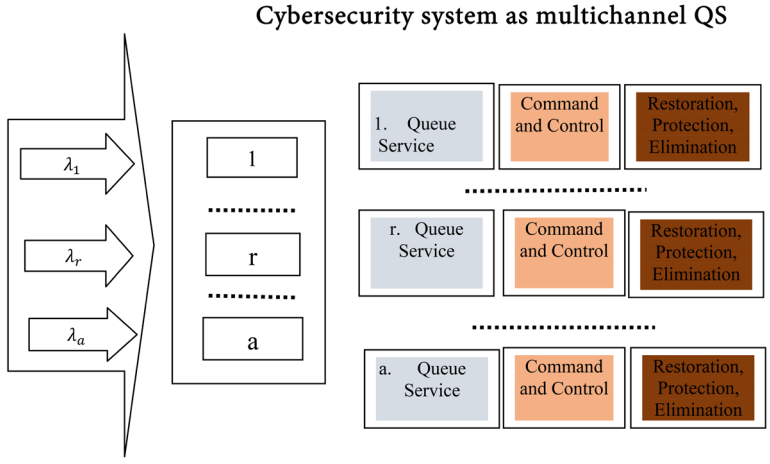

Figure 2. The block diagram of the multi-channel Queuing System under study, each channel of which is represented in the form of the Queuing System shown in **Figure 1**.

- a—number of multichannel subsystems comprising the system where $a = \overline{1, N}$;
- N—maximum number of subsystems in the information system;
- n_r—number of service channels that are being restored in each subsystem where $r = \overline{1, n}$;
- λ_r—parameter of Poisson law—intensity of cyberattacks causing failures and other disorders in service channels where $r = \overline{1, a}$;
- m_r—the number of places in the queue in the r-subsystem.
- I_r—the number of r-subsystems requests being in the service channels.
- Probability processes of restoration of service channels, as well as eliminations of consequences of cyber-impacts are described by exponential law with

the parameter μ_r, where $r = \overline{1,a}$;

- Loading intensity of service channels: $\rho_r = \lambda_r / \mu_r$;
- Total intensity of cyberthreats upon the system: $\Lambda = \sum_{r=1}^{a} \lambda_r$;
- Total intensity of restauration of service channels: $M = \sum_{r=1}^{a} \mu_r$;
- Total loading of system: $\rho = \sum_{r=1}^{a} \rho_r$.

5. Indices of Operation Efficiency of the Investigated System

For modelling purposes as main characteristics of operation efficiency of the investigated ISCI, there have been taken characteristics given below whose values are defined by the values of above listed parameters having probabilistic nature.

$p_{k_r}^a$ —total limitary probabilities of the number of channels exposed to cyberthreats.

$p_{n_r+l_r}^a$ —probability of cyber-attacks in the system ($n_r + l_r$);

p_{query}^a —total probabilistic number of discovered cyber-threats whose consequences are to be eliminated;

$p_{failure}^a$ —total probability of refusal to restore the consequences of cyber-attacks because of overload of restoration system;

Q^a —the total relative service capacity of the restoration system to restore consequences of cyber-attacks.

A^a —total absolute service capacity of the restoration system to restore the consequences of cyberattacks;

L_{queue} —total average number of cyber-attack consequences waiting for restoration of the consequences.

$L_{service}$ —average number of request orders served by QS per time unit.

L_{qs} —Total average number of cyber-incidents being in the process of elimination of their consequences as well as waiting for such process.

6. The Mathematical Model of the Investigated System of Cybersecurity

As a result of the corresponding transformations of functional relationships that describe initial basic model of multichannel QS with unlimited queue, there has been received a new operating model of the investigated system in the form of below given mathematical relationships, which describe interconnection between its input and output parameters.

1) Total limit probability while $k_r = \overline{0,n_r}$, where k_r—number of channels being cyber-attacked, and n_r—number of channels in the r-subsystem.

$$p_0^a = \sum_{r=1}^{a} p_0^r = \sum_{r=1}^{a} \left[\sum_{k=0}^{n} \left(\rho_r^k / k_r ! \right) + \left(\rho_r^{n_{r+1}} / \left(n_r ! * \left(n_r - \rho_r \right) \right) \right) * \left(1 - \left(\rho_r / n_r \right)^{m_r} \right) \right]^{-1}, \quad k_r = 0, \quad r = \overline{1,a}; \tag{1}$$

$$p_{k_r}^a = \sum_{r=1}^{a} \left(\rho_r^{k_r} / k_r \right) * p_0^r, \quad r = \overline{1,a}, \quad k_r = \overline{0,n_r}; \tag{2}$$

2) In the system ($n_r + l_r$) probability of cyberattacks, from them n_r—in the

process of restauration of ration of consequences, and waiting for such process.

$$p_{n_r+l_r}^{a} = \sum_{r=1}^{a}\left(\rho_r^{n_r+l_r} \Big/ \left(n_r^{l_r} * n_r !\right)\right) p_0^r,\ \ r=\overline{1,a},\ \ n_r \le l_r \le m_r; \tag{3}$$

3) Total probable number of detected cyberattacks whose consequences have to be eliminated.

$$\begin{aligned} p_{query}^{a} &= \sum_{r=1}^{a}\sum_{l=0}^{n_r+m_r-1} p_{n_r+1}^{r} \\ &= \sum_{r=1}^{a}\sum_{l=0}^{n_r+m_r-1}\left(\rho^{n_r}/n_r !\right) * \left(\left(1-\left(\rho_r/n_r\right)^{m_r}\right) \Big/ \left(1-\rho_r/n_r\right)\right) * p_0^r,\ \ r=\overline{1,a}; \end{aligned} \tag{4}$$

4) Total probability of refusals of consequences resulted by cyberattacks because of overloading of the restauration system.

$$p_{failure}^{a} = \sum_{r=1}^{a} p_{n_r+m_r}^{r} = \sum_{r=1}^{a} \frac{\rho^{n_r+m_r}}{n_r^{m_r} * n_r !} * p_0^r,\ \ k_r = n_r + m_r,\ \ r=\overline{1,a}; \tag{5}$$

5) Total relative zero-error capacity of restoration system of after cyberattacks.

$$Q^a = p_{service}^{a} = 1 - p_{failure}^{a} = \sum_{r=1}^{a}\left(1-\rho^{n_r+m_r} \Big/ n_r^{m_r} * n_r ! * p_0^r\right),\ \ r=\overline{1,a}; \tag{6}$$

6) Total absolute throughout capacity of the restoration system after cyberattacks.

$$A^a = \sum_{r=1}^{a}\lambda_r * Q^r = \sum_{r=1}^{a}\lambda_r * \left(1-\left(\rho^{n_r+m_r} \Big/ n_r^{m_r} * n_r !\right)\right) * p_0^r,\ \ r=\overline{1,a}; \tag{7}$$

7) Total average number of consequences of cyberattacks waiting for restauration.

$$\begin{aligned} L_{queue} &= \sum_{r=1}^{a}\sum_{i=1}^{m}\left(\rho^{n_{r+1}} \Big/ n_r * n_r !\right) \\ &* \left(\left(1-\left(\rho_r/n_r\right)^{m_r} * \left[1+m_r\left(1-\rho_r/n_r\right)\right]\right) \Big/ \left(1-\rho_r/n_r\right)^2\right) * p_0^r,\ \ r=\overline{1,a}; \end{aligned} \tag{8}$$

8) Average number of service requests being served by QS per unit time.

$$L_{service}^{a} = \sum_{r=1}^{a} A^r/\mu_r = \sum_{r=1}^{a}\rho * \left(1-\left(\rho^{n_r+m_r} \Big/ n_r^{m_r} * n_r !\right)\right) * p_0^r,\ \ r=(1,a); \tag{9}$$

9) Total average number of cyber-incidents being in the process of eliminations of their consequences as well as waiting for such process.

$$L_{qs}^{a} = L_{queue}^{a} + L_{service}^{a} \tag{10}$$

7. The Novelty of Investigation

The specific feature of the model described in the article is an attitude towards the problem that enables to develop most generalized, enlarged and scaling software model of the cybersecurity protection system, as it was said above, that is presented as a complex system consisting of certain number of multichannel subsystems of queueing service with unlimited queue exposed to different types of cyber-impacts which cause undesired consequences in the service channels.

The research has been conducted according to the assumption that all the channels of the information system in question, in its composition, along with the devices directly performing technological processes, contain complex intelligence system of command, control and protection from consequences of corres-

ponding types of cyber-impacts, and it provides with:

1) Constant monitoring aiming at detection, identification and registration of different disorders of system operation, happening as a result of ordinary causes (such as failures and restorations), as well as the result of cyber-impacts of different types that disturb entity, confidence and availability.

2) Initiating the processes of restoration of the failed devices and elimination of consequences of any probable cyber-impacts, performing by programs or tools in corresponding equipment presupposed in the service channels.

3) Possibility of information system being under joint impact of different types of cyber-threats including unauthorized access request, viruses, spam, remote login, phishing, DoS/DDoS—attacks etc. happening at random according to the familiar laws of probability distribution.

4) Presence of restoration means, corresponding to their purposes, characteristics and abilities, in the given channel presupposed cyber-impacts, as well as equipment of command for restoration of the failed service channels and elimination of consequences of cyber-impacts that assure effective operation of information system.

8. Results and Discussion

This article summarizes some of the results of research in the field of reliability and security of complex technical systems, with the aim of applying them to the study of cybersecurity problems of Information Systems of Critical Infrastructures. The results of the work contribute to the development of theoretical foundations for assessing the state of cybersecurity in order to ensure the effectiveness of their functioning in the context of cyber threats.

9. Conclusions

In the article, in accordance with the stated objectives, the following problems are solved:

- A new analytical model has been developed for the estimation of the level of cybersecurity protection of information systems, considered as complex queueing systems exposed to cyberattacks of different nature.
- As a basis of modelling of the cybersecurity system in question there has been chosen Multichannel Queuing System with unlimited queue that is well known and is widely applied in practice.

There has been made a generalization and it presupposes consideration of the abovementioned system as a constituent part of a subsystem that is a part of more generalized, enlarged and scaling system that is an aggregation of several, similar to the above described, subsystems.

- There have been received new analytical relationships reflecting dependence of values of input parameters and output characteristics of generalized, enlarged and scaling system describing its work as operation of queueing system in the conditions of cyber-impacts.

- On the basis of received new analytical relationships for different characteristics of the given generalized model, it is possible to develop software model enabling to conduct simulation work of described generalized QS under the influence of cyberattacks and evaluating different scenarios of system operation taking into consideration its specific features.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Bezkorovainy, M. and Tatuzov, A. (2014) Cybersecurity—Approaches to the Definition. Voprosi Kiberbezopasnosti, No. 1.

[2] Starovojtov, A.V. (2011) Cybersecurity as an Actual Modern Problem. *Informatization and Communication*, **6**, 4-7.

[3] Bezkorovainy, M.M., Losev, S.A. and Tatuzov, A.L. (2011) Cybersecurity in the Modern World: Terms and Content. *Informatization and Communication*, **6**, 27-32.

[4] Saati, T.L. (1965) Elements of Queuing Theory and Its Application. Sovetskoe Radio, Moscow, 510.

[5] Cherkesov, G.N. (1974) Dependability of Technical Systems with Time Redundancy. Sovetskoe Radio, Moscow, 296.

[6] Gnedenko, B.V. and Kovalenko, I.N. (2012) Introduction to Queuing Theory. LKT, 400.

[7] Feller, W. (1971) An Introduction to Probability Theory and Its Applications. Vol. 2, John Willey and Sons, New York, 766.

[8] Shubinski, I.B. (2016) Nadejnie otkazoustoichivie informacionnie sistemi. Metodi sinteza-M. Jurnal Nadejnost, 546 str.il.

[9] Klimov, S.M., Polikarpov, C.B., Rijov, B.C., Tichonov, R.I. and Shpirnja, I.V. (2019) Metodika obespechenija ustoichivosti funkcionirovanija kriticheskoi informacionni infrastrukturi v uslovijax informacionnix vozdeistvii. *Voprosi kiberbezopasnosti*, **6**, 37-48.

[10] Kondakov, C.E., Mesherjakov, T.B., Scril, C.B., Stadnik, A.H. and Suvorov, A.A. (2019) Verojtnostnoe predstavlenie uslovii sovremennogo reagirovanija na ugrozi kompiuternix atak. *Voprosi kiberbezopasnosti*, **6**, 59-68.

[11] Zaxarchenko, R.I. and Koroliov, I.D. (2019) Model funkcionirovanija avnomatizirovannoi informacionnoi sistemi v kibrprostranstve. *Voprosi kiberbezopasnosti*, **6**, 69-78.

[12] Gapanovich, V.A., Chubinskii, I.B. and Zamuchljev, A.M. (2016) Metod ozenki riskov sistemu iz raznotipnuch elementov. *Nadezhnost*, **16**, 49-53.

[13] Klimov, S.M. and Kotjchev, N.N. (2013) Metod regulirovanij riskov kompleksov sredstv avtomatizacii v uslovijch kompjyternuch atak. *Nadezhnost*, No. 2, 93-107.

[14] Chubinskii, I.B. (2012) Funkcionalnaj nadezhnost informacionnuch system. Metodu analiza/I.B Chubinskii. Oblastnaj tipografij "Pechatnui dvor", Uljnovsk, 296 s.

[15] Shamugia, R.R. (2014) On One Model of Complex Technical Queuing System with Unreliable Devices and with Time Redundancy. *International Journal of Communications, Network and System Sciences*, **7**, 257-264.

https://doi.org/10.4236/ijcns.2014.78028

[16] Shamugia, R.R. (2014) On One Model of Multichannel Queuing System with Unreliable Repairable Servers and Input Memory. *International Journal of Communications, Network and System Sciences*, **7**, 279-285. https://doi.org/10.4236/ijcns.2014.78030

[17] Shamugia, R.R. (2015) On One Analytical Model of a Probability Estimation of Quality and Efficiency of Functioning of Complex Technical Queuing Systems. *International Journal of Communications, Network and System Sciences*, **8**, 295-303. https://doi.org/10.4236/ijcns.2015.88029

[18] Shamugia, R.R. (2016) Probabilistic Model of Technical Queuing Systems with Subsystems for Detection and Recovery of Failures. *International Journal of Communications, Network and System Sciences*, **9**, 305-310. https://doi.org/10.4236/ijcns.2016.98027

[19] Shamugia, R.R. (2019) Development of the Software Application with Graphical User Interface for One Model Cyber Security. *International Journal of Communications, Network and System Sciences*, **12**, 199-208. https://doi.org/10.4236/ijcns.2019.1212014

[20] Shamugia, R.R. (2018) Development and Investigation of the Program Model of Multichannel Queueing System with Unreliable Recoverable Servers in Matlab Environment. *International Journal of Communications, Network and System Sciences*, **11**, 229-237. https://doi.org/10.4236/ijcns.2018.1111014